FRAMEWORK AGREEMENT

THIS FRAMEWORK AGREEMENT (this "Agreement") is made between the **CITY AND COUNTY OF DENVER**, a municipal corporation of the State of Colorado (the "City" or the "Customer"), and **AXON ENTERPRISE INC**., an Arizona corporation, whose address is 17800 N 85th St, Scottsdale, AZ 85255 (the "Contractor" or "Axon"), individually a "Party" and jointly "the Parties."

RECITALS

WHEREAS, the City awarded this Agreement to the Contractor for the provision and implementation of an Automatic License Plate Recognition (ALPR) system.

NOW, THEREFORE, in consideration of the mutual covenants and agreements hereinafter set forth and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the Parties incorporate the recitals set forth above and agree as follows:

1. DEFINITIONS

1.1. "City Data" means all data, information, documents, records, and materials in any format that: (i) originate from or are owned by the City; (ii) are provided by the City to the Contractor; (iii) are accessed by the Contractor from City systems, databases, or repositories; (iv) are created, developed, compiled, generated, or derived by the Contractor using, incorporating, or based upon any City-originating data; (v) contain or reference any City-originating data; or (vi) are maintained, processed, stored, or transmitted by the Contractor in connection with this Agreement and relate to City operations, services, residents, employees, or business. City Data includes all reports, analyses, summaries, compilations, derivatives, and other work products created by the Contractor that incorporate or are based upon any of the foregoing data.

1.2. "Deliverables" means any and all On-Premise Software, SaaS, Services, Products, intellectual property, documentation, materials, labor, support, maintenance, training, updates, configurations, customizations, and other outputs and outcomes provided and/or performed by the Contractor pursuant to this Agreement, whether explicitly identified in this Agreement or reasonably necessary to fulfill the Contractor's obligations hereunder. Deliverables do not include the Contractor's pre-existing intellectual property or third-party components except to the extent expressly licensed or assigned to the City under this Agreement.

1.3. "Effective Date" means the date on which this Agreement is approved and signed by the City as shown on the City's signature page.

1.4. "Exhibits" means the exhibits and attachments included with this Agreement.

1.5. "On-Premise Software" means software that the Contractor provides for the City's use that is installed and operated on City premises. For the avoidance of doubt, On-Premise Software does not include SaaS, though On-Premise Software may interface with SaaS.

1.6. "Personally Identifiable Information" or "PII" means personally identifiable information including, without limitation, any information maintained by the City about an individual that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records. PII also includes any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information. PII includes, but is not limited to, all information defined as "personally identifiable information" in Colo. Rev. Stat. §§ 24-72-501(2), 24-74-102(1), and 24-73-101(4)(b). "PII" shall also mean "personal information" as defined in Colo. Rev. Stat. § 24-73-103(1)(g).

1.7. "Product(s)" means all equipment, hardware, components, peripherals, accessories, supplies, parts, consumables, materials, and associated documentation delivered or to be delivered by the Contractor under this Agreement, including any customized, configured, or modified versions thereof, as well as any replacements, updates, or upgrades provided during the term of this Agreement.

1.8. "SaaS" means a software-as-a-service that the Contractor hosts (directly or indirectly) for the City's use. For the avoidance of doubt, SaaS does not include Services or On-Premise Software.

1.9. "Service(s)" means the technology related professional services to be performed by the Contractor as set forth in this Agreement and shall include any services or support provided by the Contractor under this Agreement.

1.10. "Specifications" refers to such technical and functional specifications for On-Premise Software, SaaS, and/or Deliverables included or referenced in an Exhibit.

1.11. "Subcontractor" means any third party engaged by the Contractor to aid in performance of the Work.

1.12. "Task Order" means a document issued in accordance with this Agreement that specifically describes additional Work to be performed.

1.13. "Work" means the process of providing, performing, implementing, maintaining, supporting, configuring, customizing, updating, delivering, and otherwise making available all Deliverables as defined in this Agreement. Work includes all efforts, labor, activities, tasks, and responsibilities required to fulfill the Contractor's obligations under this Agreement, whether specifically enumerated or reasonably implied, and shall be conducted in accordance with the standards, timeframes, and requirements set forth herein.

2. SCOPE OF WORK AND PERFORMANCE STANDARDS

2.1. Coordination with the City: The Contractor shall fully coordinate all Work performed under this Agreement with the City's Chief Information Officer ("CIO"); with other personnel formally designated by the Department of Technology Services ("TS"); or, if applicable, with a representative from another City agency, as may be expressly designated by the CIO to act on behalf of the City for purposes of this Agreement. If a third party is designated by the CIO to serve as a liaison or coordinating

entity on behalf of the City, the Contractor shall also coordinate its Work with such third party in the same manner and to the same extent as it would with City personnel.

2.2. Contractor Performance Standards: The Contractor shall diligently perform, deliver, and maintain all Deliverables specified in this Agreement. The City shall have no obligation to compensate the Contractor for any Work not expressly authorized under this Agreement. All Work shall be provided and performed in accordance with the Specifications set forth herein. The Contractor represents and warrants that it possesses the necessary expertise, capabilities, and resources to provide the Work required by this Agreement. The Contractor shall perform all obligations with reasonable professional care, skill, training, diligence, and judgment consistent with generally accepted industry standards and practices for comparable Work, and in compliance with all applicable terms, conditions, and requirements of this Agreement free from any liens, adverse claims, encumbrances, or third-party interests.

2.3. Key Personnel: If an Exhibit or Task Order identifies key personnel, the Contractor shall not reassign, replace, or remove such personnel without providing the City at least thirty (30) days' prior written notice and obtaining the City's written approval, which shall not be unreasonably withheld. Replacement personnel shall possess qualifications and experience comparable to or exceeding those of the personnel being replaced. The Contractor shall provide the City with the qualifications of any proposed replacement for review prior to assignment. The departure of key personnel without adequate replacement may, at the City's sole discretion, constitute a material breach of this Agreement.

2.4. Contractor Representations: The Contractor represents and warrants that, as of the Effective Date and throughout the Term: (i) it is not currently debarred, suspended, or proposed for debarment by any federal, state, or local government entity; (ii) there is no pending or threatened litigation, investigation, or proceeding that could materially impair the Contractor's ability to perform its obligations under this Agreement; (iii) it has not made and will not make any unlawful payments, bribes, or kickbacks in connection with obtaining or performing this Agreement; (iv) all information provided to the City during the procurement process and in connection with this Agreement is accurate and complete in all material respects; (v) it is in good standing in the state of its organization and is qualified to do business in Colorado; and (vi) it has disclosed to the City in writing any agreement, contract, or arrangement it or any of its Subcontractors currently maintains with the United States Department of Homeland Security or any component agency thereof, including the specific federal agency, the nature of the work performed, and the terms of compensation, as well as any third-party data-sharing arrangements related thereto. The Contractor shall promptly notify the City in writing if any of these representations ceases to be accurate during the Term.

2.5. Task Orders for Additional Work

2.5.1. The City may request additional Work by issuing a Task Order. All Task Orders must be signed by both Parties and shall incorporate the rates established in the Exhibits or, with the City's prior written approval, alternative rates specifically negotiated for that Task Order. Each Task Order must specify: (i) a detailed scope, quote, or order form; (ii) completion timeline; (iii) applicable pricing structure (hourly rates or fixed fee); (iv) payment schedule; and (v) a "not to exceed" amount. Task Orders shall be construed to be in addition to, supplementary to, and consistent with the provisions of this Agreement. Task Orders may be amended through a written instrument jointly prepared and signed by authorized representatives of both Parties.

2.5.2. The City maintains sole discretion regarding the execution of Task Orders and is not obligated to issue any minimum number. The Contractor is not entitled to compensation for Work not expressly authorized by this Agreement or a properly executed Task Order. Expiration or termination of this Agreement automatically terminates all associated Task Orders unless the Parties explicitly agree otherwise in writing. The City may also terminate individual Task Orders according to the termination provisions in this Agreement.

2.6. License Administration: The City may, at its sole discretion and without formal amendment, reassign, add, remove, or substitute individual licensees or authorized users under this Agreement at any time during the Term. Reassignment of existing licenses among City personnel shall not result in additional fees. Additions that increase the total number of licenses beyond the quantity then in effect shall be invoiced at the applicable per-unit rates established in the Exhibits. Reductions shall be governed by **Exhibit C**. The Contractor shall implement license changes within five (5) business days of the City's written request. If the Contractor offers alternative products or modules within its product portfolio, the City may substitute licensed products upon written notice to the Contractor, provided that (i) the Parties agree in writing to the applicable pricing for the substitute product, (ii) the substitution does not increase the Maximum Agreement Amount, and (iii) the substitution does not extend the Term. Such substitutions shall be documented by written acknowledgment of both Parties but shall not require a formal amendment.

3. AGREEMENT TERM AND RENEWAL

3.1. Term: The term of the Agreement ("Term") shall commence on April 1, 2026, and expire, unless sooner terminated, on March 31, 2027. Subject to the City's prior written authorization, the Contractor shall complete any work in progress as of the then current expiration date and the Term will extend until the work is completed or earlier terminated.

3.2. Limited Extension for Completion of Authorized Work: If, at the expiration of the Term, the Contractor is performing Work pursuant to a Task Order or other written authorization that the Parties expected would be completed prior to expiration,

the City may, in its sole discretion, provide written authorization for the Contractor to complete such Work. Upon the City's written authorization, the Term shall extend for the period specified in the City's authorization to enable completion of the specifically identified Work and submission and processing of final invoices. Any such extension shall not constitute authorization for any new Work or general renewal of this Agreement. The City may terminate any such extension in accordance with the termination provisions herein**.**

3.3. **Timely Renewal and Extension Documentation**: To facilitate the City's contract amendment process and ensure continuity of services, the Contractor shall provide the City with all required order forms, pricing information, and renewal documentation no later than one hundred twenty (120) days prior to the expiration of the Term. The Contractor shall negotiate any extension or renewal of this Agreement in good faith and may not introduce changes to the legal terms and conditions of this Agreement through order forms, quotes, or other renewal documentation. If the Contractor does not intend to renew or extend the Term of this Agreement, the Contractor shall provide written notice to the City no later than one hundred eighty (180) days prior to the expiration of the Term.

4. COMPENSATION AND PAYMENT

4.1. **Fees**: The City shall pay, and the Contractor shall accept as the sole compensation for Work rendered and costs incurred under this Agreement the fees described in the attached Exhibits. Amounts billed may not exceed rates set forth in the Exhibits and will be made in accordance with any agreed upon payment milestones.

4.2. **Reimbursement Expenses**: There are no reimbursable expenses allowed under this Agreement. All the Contractor's expenses are contained in the budget as described in the Exhibits. The City will not be obligated to pay the Contractor for any other fees, costs, expenses, or charges of any nature that may be incurred and paid by the Contractor in performing their obligations under this Agreement including but not limited to personnel costs, benefits, contract labor, overhead, administrative costs, operating costs, supplies, equipment, and out-of-pocket expenses.

4.3. **Invoicing**: The Contractor must submit an invoice which shall include the City contract number, clear identification of the Work that has been completed, and other information reasonably requested by the City. Payment on all uncontested amounts shall be made in accordance with the City's Prompt Payment Ordinance, D.R.M.C §§ 20-107 et seq. To the extent any exhibit, attachment, or addendum to this Agreement, including any document governing the scope, ordering, or delivery of Work, sets forth additional invoicing or billing requirements, such requirements shall supplement the foregoing; provided, however, that no such additional requirements shall modify or conflict with the City's obligations under the Prompt Payment Ordinance.

4.4. **Maximum Agreement Amount**

4.4.1. Notwithstanding any other provision of this Agreement, the City's total financial obligation shall not exceed One Hundred Fifty Thousand Dollars

($150,000.00) (the "Maximum Agreement Amount"). The City has no obligation to execute any amendments or authorizations for additional Work beyond that specifically described in the attached Exhibits. Any Work performed by the Contractor that exceeds the scope defined in the attached Exhibits, or that would cause the Maximum Agreement Amount to be exceeded, shall be performed at the Contractor's sole risk and expense and without authorization under this Agreement. The Maximum Agreement Amount includes all fees, costs, expenses, and other charges that may be incurred by the Contractor in fulfilling its obligations hereunder.

4.4.2. The City's payment obligation, whether direct or contingent, extends only to funds appropriated annually by the Denver City Council, paid into the Treasury of the City, and encumbered for the purpose of this Agreement. The City does not by this Agreement irrevocably pledge present cash reserves for payment or performance in future fiscal years. This Agreement does not and is not intended to create a multiple-fiscal year direct or indirect debt or financial obligation of the City.

4.5. Taxes, Charges, and Penalties: The City shall not be liable for the payment of taxes, late charges, or penalties of any nature other than the compensation stated herein, except for any additional amounts which the City may be required to pay under D.R.M.C. §§ 20-107 to -115.

5. CONTRACTOR STATUS AND SUBCONTRACTING

5.1. Independent Status: The Contractor is an independent contractor retained to perform professional or technical services for limited periods of time. Neither the Contractor nor any of its employees are employees or officers of the City under Chapter 18 of the Denver Revised Municipal Code, or for any purpose whatsoever. Nothing contained in this Agreement shall be construed as creating any agency, partnership, joint venture, or other form of joint enterprise, or employment relationship between the Parties.

5.2. Assignment and Subcontracting: The Contractor shall not sell, transfer, assign, subcontract performance obligations, or otherwise dispose of this Agreement or any portion thereof, including any right, title, or interest therein, without the City's prior written consent. The City shall not unreasonably withhold approval of an assignment when the Contractor is in full compliance with this Agreement and the proposed assignee, in the City's opinion, possesses sufficient business experience, aptitude, and financial resources to perform its obligations under this Agreement. The City may, at its reasonable discretion, approve the assignment, subcontract, or transfer in writing, deny it, or refer the matter to the City's governing bodies for approval. The City may provide its written approval of an assignment without requiring a formal amendment to this Agreement. Such written approval may be delivered through a consent letter or other written communication, provided it explicitly references this Agreement. Any approved assignee shall be subject to all terms and conditions of this Agreement and

other supplemental contractual documents; however, no approval by the City shall obligate the City beyond the provisions of this Agreement. Any assignment or subcontracting without the City's consent shall be ineffective and void and shall constitute grounds for termination of this Agreement by the City. Should unauthorized assignment or subcontracting occur, the Contractor shall remain responsible to the City, and no contractual relationship shall be created between the City and any subcontractor or assignee. This provision shall also apply to any assignment of this Agreement due to change in ownership of the Contractor, and the Contractor shall notify the City in writing of any assignment due to change in ownership within thirty (30) days of such change.

6. TERMINATION

6.1. Termination for Breach: Either Party may terminate this Agreement for material breach by providing 30 days written notice detailing the breach, unless the breaching party cures the breach within that period. Termination is effective immediately if the breach cannot be cured.

6.2. City Termination Without Cause: The City may terminate this Agreement, or a specific Deliverable under this Agreement, without cause with 60 days written notice. Upon termination without cause, the City shall pay the Contractor for: (i) all completed and accepted Work performed through the effective date of termination; and (ii) all non-cancelable commitments reasonably incurred by the Contractor prior to receiving notice of termination. The City has no obligation to pay for subscription years, licensing fees, or support costs beyond the effective date of termination. Notwithstanding § 14.1 of **Exhibit F**, no termination fee, MSRP differential, or clawback of any kind shall be owed by the City upon termination under this Section.

6.3. Immediate Termination for Criminal Activity: The City may immediately terminate if the Contractor or its personnel are convicted of or admit to criminal offenses including bribery, fraud, theft, antitrust violations, or similar crimes related to business activities. The City may also suspend performance during investigations of such conduct.

6.4. Termination for Public Interest or Lack of Appropriation: If this Agreement ceases to further the public interest of the City, or if the City fails to appropriate the necessary funding to continue this Agreement, the City, in its discretion, may terminate this Agreement in whole or in part. A determination that this Agreement should be terminated in the public interest or for lack of appropriation shall not be equivalent to a City right to terminate for convenience or without cause. Upon such termination, the City will pay the Contractor for the percentage of satisfactorily completed and accepted Work, less previous payments.

6.5. Post-Termination Obligations: Upon termination of this Agreement, the Contractor shall have no claim against the City by reason of, or arising out of, incidental or relating to termination, except for compensation for satisfactorily completed Work. The Contractor must return all City property upon request or termination.

7. **EXAMINATION OF RECORDS AND AUDITS**: Any authorized agent of the City, including the City Auditor or his or her representative, has the right to access, and the right to examine, copy and retain copies, at City's election in paper or electronic form, any pertinent books, documents, papers and records related to the Contractor's performance pursuant to this Agreement, provision of any goods or services to the City, and any other transactions related to this Agreement. The Contractor shall cooperate with City representatives and City representatives shall be granted access to the foregoing documents and information during reasonable business hours and until the latter of three (3) years after the final payment under this Agreement or expiration of the applicable statute of limitations. When conducting an audit of this Agreement, the City Auditor shall be subject to government auditing standards issued by the United States Government Accountability Office by the Comptroller General of the United States, including with respect to disclosure of information acquired during the course of an audit. No examination of records and audits pursuant to this paragraph shall require the Contractor to make disclosures in violation of state or federal privacy laws. The Contractor shall at all times comply with D.R.M.C. § 20-276.

8. **INSURANCE**

   8.1. **General Conditions**: The Contractor agrees to secure, at or before the time of execution of this Agreement, the following insurance covering all operations, goods or services provided pursuant to this Agreement. The Contractor shall keep the required insurance coverage in force at all times during the term of this Agreement, including any extension thereof, and during any warranty period. The required insurance shall be underwritten by an insurer licensed or authorized to do business in Colorado and rated by A.M. Best Company as "A-VIII" or better. Each policy shall require notification to the City in the event any of the required policies be canceled or non-renewed before the expiration date thereof. Such written notice shall be sent to the parties identified in the Notices Section of this Agreement. Such notice shall reference the City contract number listed on the signature page of this Agreement. Said notice shall be sent thirty (30) days prior to such cancellation or non-renewal unless due to non-payment of premiums for which notice shall be sent ten (10) days prior. If such written notice is unavailable from the insurer, the Contractor shall provide written notice of cancellation, non-renewal and any reduction in coverage to the parties identified in the Notices Section by certified mail, return receipt requested within three (3) business days of such notice by its insurer(s) and referencing the City's contract number. The Contractor shall be responsible for the payment of any deductible or self-insured retention. The insurance coverages specified in this Agreement are the minimum requirements, and these requirements do not lessen or limit the liability of the Contractor. The Contractor shall maintain, at its own expense, any additional kinds or amounts of insurance that it may deem necessary to cover its obligations and liabilities under this Agreement.

   8.2. **Proof of Insurance**: The Contractor may not commence Work relating to this Agreement prior to placement of coverages required under this Agreement. The

Contractor certifies that the certificate of insurance attached as **Exhibit B**, preferably an ACORD form, complies with all insurance requirements of this Agreement. The City requests that the City's contract number be referenced on the certificate of insurance. The City's acceptance of a certificate of insurance or other proof of insurance that does not comply with all insurance requirements set forth in this Agreement shall not act as a waiver of the Contractor's breach of this Agreement or of any of the City's rights or remedies under this Agreement. In the event of a claim, the City's Risk Management Office may require additional proof of insurance, including but not limited to policies and endorsements.

8.3. **Additional Insureds**: For Commercial General Liability, Auto Liability and Excess Liability/Umbrella (if required), the Contractor and Subcontractor's insurer(s) shall include the City and County of Denver, its elected and appointed officials, employees, and volunteers as additional insured.

8.4. **Waiver of Subrogation**: For all coverages required under this Agreement, with the exception of Professional Liability – if required, the Contractor's insurer shall waive subrogation rights against the City.

8.5. **Subcontractors and Subconsultants**: The Contractor shall confirm and document that all Subcontractors and subconsultants (including independent contractors, suppliers or other entities providing goods or services required by this Agreement) procure and maintain coverage as approved by the Contractor and appropriate to their respective primary business risks considering the nature and scope of services provided.

8.6. **Workers' Compensation and Employer's Liability Insurance**: The Contractor shall maintain the coverage as required by statute for each work location and shall maintain Employer's Liability insurance with limits of $100,000 per occurrence for each bodily injury claim, $100,000 per occurrence for each bodily injury caused by disease claim, and $500,000 aggregate for all bodily injuries caused by disease claims.

8.7. **Commercial General Liability**: The Contractor shall maintain a Commercial General Liability insurance policy with minimum limits of $1,000,000 for each bodily injury and property damage occurrence, $2,000,000 products and completed operations aggregate (if applicable), and $2,000,000 policy aggregate.

8.8. **Automobile Liability**: The Contractor shall maintain Automobile Liability with minimum limits of $1,000,000 combined single limit applicable to all owned, hired, and non-owned vehicles used in performing Work under this Agreement.

8.9. **Professional Liability (Errors & Omissions)**: The Contractor shall maintain minimum limits of $1,000,000 per claim and $1,000,000 policy aggregate limit. The policy shall be kept in force, or a Tail policy placed, for three (3) years for all contracts except construction contracts for which the policy or Tail shall be kept in place for eight (8) years.

8.10. **Cyber Liability**: The Contractor shall maintain Cyber Liability coverage with minimum limits of $1,000,000 per occurrence and $1,000,000 policy aggregate

covering claims involving privacy violations, information theft, damage to or destruction of electronic information, intentional and/or unintentional release of private information, alteration of electronic information, extortion and network security. If Claims Made, the policy shall be kept in force, or a Tail policy placed, for three (3) years.

9. BREACH AND REMEDIES: This Section establishes the general framework governing breach, cure procedures, and remedies applicable to this Agreement. The provisions herein supplement and work in conjunction with specific remedial provisions set forth elsewhere in this Agreement, including but not limited to the termination rights, the indemnification and limitation of liability provisions, the Security Breach obligations, and the accessibility remediation requirements. Where such specific provisions exist, they shall govern with respect to their subject matter, and this Section shall provide additional and cumulative remedies unless expressly stated otherwise. The Parties acknowledge that the remedies specified throughout this Agreement, including those enumerated in this Section, are not intended to be exclusive but rather to provide the non-breaching Party with a comprehensive array of options to protect its interests and ensure proper performance. The Parties' rights under this Section are in addition to, and not in lieu of, any other rights or remedies available under applicable law, including the City's sovereign prerogatives and its authority to protect the public interest.

9.1. Definition of Breach: A breach occurs when either Party fails to perform any material obligation under this Agreement in a timely or satisfactory manner. The institution of bankruptcy, insolvency, reorganization, or similar proceedings by or against the Contractor, or the appointment of a receiver or similar officer for the Contractor or its property, which is not vacated or fully stayed within thirty (30) days, shall also constitute a breach by the Contractor. For purposes of this Section, a failure to perform that qualifies as an Excusable Delay under this Agreement shall not constitute a breach, provided the delayed Party promptly notifies the other Party and provides reasonable documentation of the Excusable Delay.

9.2. Notice and Cure: Upon breach, the non-breaching Party shall provide written notice specifying the breach. The breaching Party shall have thirty (30) days after receipt of such notice to cure the breach at its sole expense, unless the breach cannot be cured, in which case the non-breaching Party may exercise its remedies immediately. Notwithstanding the foregoing, the City may immediately terminate this Agreement or exercise any other remedy herein without prior notice or cure period if: (i) the Contractor's breach poses an imminent threat to public health, safety, or welfare; (ii) the circumstances described in Section 6.3 exist; (iii) the Contractor abandons performance; or (iv) the Contractor commits a Security Breach as defined herein, provided that the notification and remediation requirements of this Agreement shall remain applicable. If, after such immediate termination, the City determines that the grounds for immediate action did not exist, the termination shall be treated as a

termination without cause under this Agreement, and the Parties' rights and obligations shall be as set forth therein.

9.3. City's Remedies: If the Contractor fails to cure a breach within the applicable cure period, the City shall have all remedies listed in this Section in addition to all other remedies available under this Agreement or at law. All remedies are cumulative and not exclusive, and the City may exercise any or all such remedies concurrently or consecutively.

9.3.1. **Withhold or Deny Payment**: Notwithstanding the payment timelines herein, the City may withhold any payment reasonably related to the breach until the breach is cured or may deny payment for Work not performed or improperly performed. Any denial of payment shall be commensurate with the value of obligations not performed or the diminution in value to the City. The City shall exercise any right to withhold payment within ninety (90) days of discovering the basis for withholding.

9.3.2. **Suspend Performance**: The City may suspend the Contractor's performance with respect to all or any portion of the Work without entitling the Contractor to any adjustment in price, cost, or schedule. The Contractor shall promptly cease Work and incurring costs in accordance with the City's directive, and the City shall not be liable for costs the Contractor incurs after such suspension.

9.3.3. **Procure Replacement Services**: The City may procure from third parties replacement or substitute Work as cover, and the Contractor shall remain liable for any reasonable excess costs the City incurs. The City may offset such excess costs against any amounts due or that may become due to the Contractor.

9.3.4. **Demand Removal of Personnel**: The City may demand removal of any of the Contractor's employees, agents, or Subcontractors whom the City reasonably deems unqualified, unprofessional, unsuitable, or whose continued involvement the City determines to be contrary to the public interest. The Contractor shall comply within five (5) business days at no additional cost to the City.

9.3.5. **Intellectual Property Remedies**: If any Work infringes, or if the City reasonably determines that any Work is likely to infringe, any intellectual property right, the Contractor shall, at the City's election and the Contractor's sole expense: (i) secure for the City the right to continue using such Work; (ii) replace or modify the Work to render it non-infringing without material degradation of functionality; or (iii) remove the infringing Work and refund to the City all amounts paid for such Work, prorated over the remaining Term.

9.3.6. **Setoff and Damages**: The Contractor shall remain liable to the City for any damages sustained by the City in connection with any breach, subject to the limitations set forth in Section 9.2. The City may setoff against any amounts due or that may become due to the Contractor any damages, costs, expenses, or other

sums the Contractor owes the City, and may withhold any amount the City reasonably deems necessary to protect against loss, including loss resulting from outstanding liens or excess procurement costs, until the exact amount of damages is determined.

9.3.7. **Audit-Discovered Breaches**: If any audit conducted pursuant to Section 7 reveals that the Contractor has overbilled the City, materially misrepresented its performance, or otherwise obtained payment for Work not properly performed, the Contractor shall immediately refund such amounts to the City with interest at the rate specified in D.R.M.C. § 20-107 et seq. from the date of overpayment. The City may setoff such amounts against any payments due or that may become due to the Contractor.

9.3.8. **Step-In Rights**: In the event of the Contractor's material breach, abandonment of performance, or insolvency, and to the extent necessary to maintain continuity of critical City operations, the City or its designee may, upon reasonable notice (or without notice if the circumstances present an imminent threat to public health, safety, or the security of City Data), access the Contractor's systems, tools, and environments solely to the extent required to maintain, operate, or transition the Work. The Contractor shall cooperate with such access and shall not impede, disable, or restrict the City's ability to access City Data or maintain service operations during any transition period. This right is in addition to, and not in lieu of, the City's rights under Section 9.3.3.

9.4. **Post-Termination Obligations**: Upon termination for breach, the Contractor shall comply with all post-termination obligations set forth in Section 6.5. In addition, at the City's request, the Contractor shall assign to the City all of the Contractor's rights, title, and interest in any outstanding orders or subcontracts related to the terminated Work. Notwithstanding anything to the contrary, the City shall only pay the Contractor for Work accepted by the City as of the date of termination. Any costs incurred by the Contractor to cure breaches, redo Work, or otherwise remedy performance deficiencies shall be at the Contractor's sole expense and shall not increase the Maximum Agreement Amount.

9.5. **Contractor's Remedies**: If the City materially breaches this Agreement and fails to cure such breach within thirty (30) days after receiving written notice specifying the breach, the Contractor may, following exhaustion of the administrative hearing process set forth herein, pursue such remedies as are available at law or in equity. If the City's breach involves failure to pay undisputed amounts when due, the Contractor may suspend performance after providing an additional fifteen (15) days' written notice, and the Contractor's obligation to continue performing shall be limited to Work for which the City has paid or for which payment is not disputed. The Contractor's monetary remedies shall be limited to direct damages actually incurred and shall exclude consequential, special, incidental, or punitive damages; provided that if the

City materially breaches its payment obligations under Section 4, the Contractor may also recover reasonable attorneys' fees incurred in collecting such amounts.

9.6. Equitable Relief: The Parties acknowledge that breach of the confidentiality, data protection, intellectual property, or personnel provisions of this Agreement may cause irreparable harm for which monetary damages are an inadequate remedy. Accordingly, either Party may seek injunctive relief or specific performance for such breaches without posting bond and without proving actual damages, in addition to any other available remedies.

9.7. Survival: The rights and remedies set forth in this Section shall survive expiration or termination of this Agreement.

10. INDEMNIFICATION AND LIABILITY

10.1. Defense and Indemnification

10.1.1. The Contractor hereby agrees to defend, indemnify, reimburse and hold harmless City, its appointed and elected officials, agents and employees for, from and against all liabilities, claims, judgments, suits or demands for damages to persons or property arising out of, resulting from, or relating to the Work performed under this Agreement ("Claims"), unless such Claims have been specifically determined by the trier of fact to be the sole negligence or willful misconduct of the City. This indemnity shall be interpreted in the broadest possible manner to indemnify City for any acts or omissions of the Contractor or its Subcontractors either passive or active, irrespective of fault, including City's concurrent negligence whether active or passive, except for the sole negligence or willful misconduct of City.

10.1.2. The Contractor's duty to defend and indemnify City shall arise at the time written notice of the Claim is first provided to City regardless of whether Claimant has filed suit on the Claim. The Contractor's duty to defend and indemnify City shall arise even if City is the only party sued by claimant and/or claimant alleges that City's negligence or willful misconduct was the sole cause of claimant's damages.

10.1.3. The Contractor will defend any and all Claims which may be brought or threatened against City and will pay on behalf of City any expenses incurred by reason of such Claims including, but not limited to, court costs and attorney fees incurred in defending and investigating such Claims or seeking to enforce this indemnity obligation. Such payments on behalf of City shall be in addition to any other legal remedies available to City and shall not be considered City's exclusive remedy.

10.1.4. Insurance coverage requirements specified in this Agreement shall in no way lessen or limit the liability of the Contractor under the terms of this indemnification obligation. The Contractor shall obtain, at its own expense, any additional insurance that it deems necessary for the City's protection.

10.1.5. The Contractor shall indemnify, save, and hold harmless the indemnified parties, against any and all costs, expenses, claims, damages, liabilities, and other amounts (including attorneys' fees and costs) incurred by the indemnified parties in relation to any claim that any Work provided by the Contractor under this Agreement (collectively, "IP Deliverables"), or the use thereof, infringes a patent, copyright, trademark, trade secret, or any other intellectual property right. The Contractor's indemnification obligations under this Section shall not apply to infringement arising solely from: (i) the City's combination of the IP Deliverables with products, systems, or methods not provided, specified, or approved by the Contractor; (ii) the City's modification of the IP Deliverables contrary to the Contractor's instructions or specifications; or (iii) the City's use of the IP Deliverables in a manner not contemplated by this Agreement or the applicable documentation, provided that such non-contemplated use was not reasonably foreseeable by the Contractor. This defense and indemnification obligation shall survive the expiration or termination of this Agreement.

10.2. **Limitation of Liability**: To the extent permitted by law, and subject to the exceptions below, the Contractor's total aggregate liability to the City under or relating to this Agreement shall not exceed five million dollars ($5,000,000). This limitation applies to all damages of any kind, including direct, indirect, consequential, special, incidental, punitive, and exemplary damages, whether arising in contract, tort, strict liability, or otherwise.

10.3. **Colorado Governmental Immunity Act**: The Parties hereto understand and agree that the City is relying upon, and has not waived, the monetary limitations and all other rights, immunities and protection provided by the Colorado Governmental Act, Colo. Rev. Stat. § 24-10-101 et seq.

11. COMPLIANCE WITH LAWS AND POLICIES

11.1. **General Compliance**: The Contractor shall comply with all applicable federal, state, and local laws, codes, rules, and regulations, including those of the United States, the State of Colorado, and the City and County of Denver. This includes, without limitation, the City's Charter, ordinances, public health orders, executive orders, and any other governing authorities relevant to the Contractor's performance under this Agreement. All such requirements are incorporated herein by reference to the extent applicable. Contractor personnel accessing City facilities shall adhere to City policies concerning facility access, use, and conduct. Upon request, the City shall provide the Contractor with copies of such policies.

11.2. **Compliance with Denver Wage Laws**: To the extent applicable to the Contractor's provision of Services hereunder, the Contractor shall comply with, and agrees to be bound by, all rules, regulations, requirements, conditions, and City determinations regarding the City's Minimum Wage and Civil Wage Theft Ordinances, D.R.M.C. §§ 58-1 to -26, including, but not limited to, the requirement that every covered worker shall be paid all earned wages under applicable state, federal, and city

law in accordance with the foregoing D.R.M.C. Sections. By executing this Agreement, the Contractor expressly acknowledges that the Contractor is aware of the requirements of the City's Minimum Wage and Civil Wage Theft Ordinances and that any failure by the Contractor, or any other individual or entity acting subject to this Agreement, to strictly comply with the foregoing D.R.M.C. Sections shall result in the penalties and other remedies authorized therein.

12. INFORMATION SECURITY AND DATA PROTECTION

12.1. Compliance with Data Protection Laws: The Contractor recognizes and agrees that: (i) City Data is valuable property of the City; (ii) City Data may include Confidential Information, protected, sensitive, or regulated data, and trade secrets of the City; and (iii) the City has dedicated substantial resources to collecting, managing, protecting, and compiling City Data. The Contractor recognizes and agrees that City Data may contain PII, as defined below, or other sensitive information, even if the presence of such information is not labeled or disclosed. If the Contractor receives access to City Data, the Contractor shall comply with all applicable federal, state, and local data protection laws, regulations, and industry standards relevant to their performance under this Agreement, including but not limited to Colo. Rev. Stat. §§ 24-73-101 et seq. At a minimum, the Contractor shall implement and maintain reasonable administrative, physical, technical, and procedural safeguards appropriate to the nature of the City Data disclosed. These safeguards must include clearly defined authorization processes, industry-standard security methods, and reasonable access restrictions to ensure the confidentiality, integrity, and availability of all City Data, protecting such data from unauthorized access, use, modification, disclosure, or destruction, and guarding against anticipated threats or hazards to its security or integrity. The Contractor shall also comply with the terms and conditions in the attached **Exhibit C**, Information Technology Provisions. The operational security standards, audit requirements, and technical controls set forth in **Exhibit C** supplement and implement the data protection obligations of this Section. In the event of conflict between this Section and **Exhibit C**, the provision imposing the greater protection for City Data shall govern. Any Exhibit or external term hereto may not waive or modify the Contractor's legal obligations to protect City Data in compliance with applicable law. The Contractor shall not share, transfer, grant access to, or otherwise make available any City databases, City Data, or technology access provided under this Agreement to the United States Department of Homeland Security or its immigration enforcement partners, except pursuant to a subpoena, judicial warrant, or court order, or as otherwise required by applicable law. Upon receipt of any request from the Department of Homeland Security or its immigration enforcement partners for access to City Data or City technology systems, the Contractor shall promptly notify the City before any disclosure and cooperate with the City's right to intervene, consistent with the procedures set forth in Section 12.4.

12.2. **Personal Information Protection**: As required by D.R.M.C. § 28-251 and Colo. Rev. Stat. § 24-74-102 et seq., the Contractor, including its employees, agents, and Subcontractors, shall not share any Personal Identifying Information (PII), as defined in Colo. Rev. Stat. § 24-74-102, with third parties for purposes of investigating for, participating in, cooperating with, or assisting in federal immigration enforcement, including enforcement of civil immigration laws and 8 U.S.C. §§ 1325 or 1326, except as required by applicable federal or state law or to comply with a judge-signed or magistrate-signed subpoena, warrant, or order. The Contractor shall not collect or disseminate individually identifiable information regarding national origin, immigration status, citizenship status, or place of birth except as expressly required by applicable federal, state, or local law. If the Contractor is granted direct access to any City database or automated network containing PII, the Contractor shall execute annually on behalf of itself and its employees a certification in the form provided by the City confirming compliance with the obligations set forth in this section, which requirement shall remain in effect for the duration of such access. If the Contractor engages any Subcontractors that require direct access to City databases or automated networks containing PII, the Contractor shall require such Subcontractors to execute and deliver the certification to the City annually for the duration of their access.

12.3. **Security Breach and Remediation**

12.3.1. **Security Breach Notification and Response**: Upon becoming aware or reasonably suspecting that a Security Breach has occurred, the Contractor shall: (i) provide initial notification to the City within forty-eight (48) hours, followed by a detailed written report within seventy-two (72) hours to Privacy@denvergov.org, ATTN: CCD Data Protection Officer; (ii) cooperate fully with the City regarding data recovery, required lawful notices, investigations, and remediation efforts; (iii) preserve and provide to the City all information and documentation relevant to the Security Breach; (iv) take immediate steps to contain and mitigate the Security Breach and prevent further unauthorized access or disclosure; and (v) conduct or commission a prompt forensic investigation to determine the cause, scope, and impact of the Security Breach. For purposes of this Section, "Security Breach" means any event that compromises the security, confidentiality, integrity, or availability of City Data, including but not limited to: (a) unauthorized or unlawful acquisition, access, use, disclosure, alteration, or destruction of City Data; or (b) loss, theft, or other compromise of systems or media containing City Data.

12.3.2. **Remediation**: The Contractor shall implement and maintain a comprehensive program for managing actual Security Breaches. Upon discovery of a Security Breach, the Contractor shall take immediate steps to contain and mitigate the Security Breach and prevent further unauthorized access or disclosure. The Contractor shall cooperate fully with the City and law enforcement agencies, when applicable, regarding data recovery, required lawful notices,

investigations, and remediation efforts. The Contractor shall preserve and provide to the City prompt access to all information, documentation, and records relevant to the Security Breach as the City may reasonably request. The Contractor may redact information that relates solely to other customers and has no bearing on the City's Security Breach, provided that the Contractor shall not redact: (i) any information concerning the Contractor's security practices, policies, procedures, or infrastructure; (ii) information concerning the root cause or attack vector of the Security Breach; (iii) information concerning the Contractor's incident response; or (iv) information necessary for the City to assess the scope and impact of the Security Breach on City Data. Any information provided under this Section shall be subject to the confidentiality obligations of this Agreement, and the City shall use reasonable efforts to protect the Contractor's proprietary information from unnecessary disclosure.

12.3.3. **Financial Responsibility**: The Contractor shall indemnify, defend, and hold the City harmless from and against all claims, liabilities, costs, expenses, and damages, including reasonable attorneys' fees, arising from or related to any Security Breach caused by the Contractor's negligent, reckless, or intentional acts or omissions, except to the extent such Security Breach is caused solely by the City's negligent acts or omissions. The Contractor shall bear all costs associated with Security Breach notification, investigation, remediation, and any legally required credit monitoring or identity protection services for affected individuals.

12.4. **Response to Legal Orders for City Data**: If the Contractor is required by a court of competent jurisdiction or administrative body to disclose City Data, the Contractor shall first notify the City and, prior to any disclosure, cooperate with the City's reasonable requests in connection with the City's right to intervene, quash, or modify the legal order, demand, or request, and upon request, provide the City with a copy of its response. Upon notice, the City will promptly coordinate with the Contractor regarding the preservation and disposition of any City Data and records relevant to any current or anticipated litigation. If the City receives a subpoena, legal order, or other legal demand seeking data maintained by the Contractor, the City will promptly provide a copy to the Contractor. Upon notice and if required by law, the Contractor shall promptly provide the City with copies of its data required for the City to meet its necessary disclosure obligations.

13. DIGITAL ACCESSIBILITY REQUIREMENTS

13.1. **Accessibility Standards**: To the extent required by law, the Contractor shall comply with the Accessibility Standards for Individuals with a Disability, as adopted by the Colorado Office of Information Technology under Colo. Rev. Stat. § 24-85-103 (the "Accessibility Standards"), and with the accessibility requirements applicable to the City as a public entity under Title II of the Americans with Disabilities Act, 42 U.S.C. § 12131 et seq., and its implementing regulations, including applicable web and mobile application accessibility standards.

13.2. **Remediation Requirements**: The City reserves the right, at its sole discretion, to engage a third-party evaluator to determine whether the Contractor is in compliance with the Accessibility Standards. The Contractor shall promptly address and resolve any accessibility non-compliance issues identified at no additional cost to the City. Upon the City's reasonable determination that accessibility issues exist, the Contractor shall develop a comprehensive remediation plan with specific timelines, subject to City approval. Accessibility issues shall be classified as high-priority fixes, and insufficient progress toward compliance with the Accessibility Standards as outlined in the approved remediation plan shall constitute a material breach of this Agreement, potentially resulting in termination or non-renewal.

13.3. **Accessibility Indemnification**: The Contractor shall indemnify, save, hold harmless, and assume liability on behalf of the City, its officers, employees, agents, and assignees for all costs, expenses, claims, damages, liabilities, court awards, and other amounts, including attorneys' fees and related costs, incurred by the indemnified parties in relation to the Contractor's noncompliance with the Accessibility Standards. For purposes of this Section, City employees are considered third parties.

14. CONFIDENTIAL INFORMATION

14.1. General Confidentiality Obligations

14.1.1. **Definition**: "Confidential Information" refers to any data or information, in any form, that is not subject to disclosure under the Colorado Open Records Act (CORA), Colo. Rev. Stat. §§ 24-72-201 et seq., and that is: (i) identified at the time of disclosure as confidential, proprietary, or otherwise protected; or (ii) that a reasonable person would understand to be confidential given the nature of the information and the circumstances of its disclosure. For the avoidance of doubt, all City Data as defined in this Agreement shall be deemed Confidential Information of the City without any requirement of marking or identification at the time of disclosure. Either Party ("Disclosing Party") may provide such information to the other ("Receiving Party") under this Agreement. This Agreement conveys no ownership or license rights in the Confidential Information.

14.1.2. **Use and Disclosure Restrictions**: The Receiving Party shall not disclose, reproduce, or use the Disclosing Party's Confidential Information except as reasonably necessary to perform its obligations under this Agreement, and only to its employees, agents, consultants, or Subcontractors who require access for performance and are bound by written confidentiality obligations no less restrictive than those set forth herein. If compelled by law, regulation, or legal process other than CORA to disclose Confidential Information, the Receiving Party shall provide the Disclosing Party with prompt written notice sufficient to allow the Disclosing Party to seek a protective order or other appropriate remedy, shall cooperate with the Disclosing Party's reasonable efforts to resist or narrow

the scope of disclosure, and shall disclose only the minimum information legally required.

14.1.3. **Exceptions**: Confidential Information does not include information that the Receiving Party can clearly demonstrate by competent evidence: (i) was lawfully in its possession prior to disclosure by the Disclosing Party; (ii) became publicly available through no breach of this Agreement; (iii) was independently developed without reference to the Disclosing Party's Confidential Information; or (iv) was lawfully obtained from a third party under no duty of confidentiality.

14.1.4. **Personally Identifiable Information**: The foregoing exceptions shall not apply to City Data containing PII, which shall remain subject to the full data protection and confidentiality obligations of this Agreement regardless of whether any individual data element within such information is, or becomes, publicly available through any means.

14.1.5. **Residual Knowledge**: Nothing in this Section shall restrict either Party's personnel from using general knowledge, skills, ideas, concepts, or techniques retained in unaided memory and gained through experience during the performance of this Agreement, provided that such use does not involve the disclosure or reproduction of Confidential Information in any tangible form.

14.1.6. **Survival**: The obligations set forth in this Section 14 survive expiration or termination of this Agreement; provided, however, that obligations with respect to City Data, Personally Identifiable Information, and trade secrets shall survive in perpetuity, and obligations with respect to all other Confidential Information shall survive for a period of five (5) years following expiration or termination.

14.2. **Colorado Open Records Act**: Nothing in this Agreement restricts the City's ability to comply with applicable laws or legal processes related to public disclosure. The Parties acknowledge that the Colorado Open Records Act (CORA), Colo. Rev. Stat. §§ 24-72-201 et seq., governs public disclosure of City records, and that materials exchanged hereunder, including Confidential Information, may be subject to disclosure thereunder. Upon receiving a disclosure request, the City shall promptly notify the Contractor, allowing an opportunity to object and identify the legal basis for withholding. In the event of legal action to compel disclosure, the Contractor shall either intervene to assert its claims or waive its objection. If the matter remains unresolved, the City shall submit the disputed material to a court for judicial determination. The Contractor further agrees to defend, indemnify, and save and hold harmless the City, its officers, agents, and employees, from any claim, damages, expense, attorneys' fees, or costs arising out of the Contractor's intervention to protect and assert its claim of privilege against disclosure under this Section.

15. **DEPARTMENT OF PUBLIC SAFETY IT PROVISIONS**: The Parties acknowledge and agree that the Department of Public Safety Information Technology Provisions ("DPS IT Provisions"), attached as **Exhibit D**, are hereby incorporated into this Agreement. The DPS IT Provisions govern all technology, software, hardware, systems, services, interfaces, data

exchanges, security requirements, and related deliverables procured, implemented, supported, or used under this Agreement. Any matters relating to the interpretation or application of the DPS IT Provisions shall be resolved in accordance with the Order of Precedence set forth within this Agreement.

16. **CRIMINAL JUSTICE INFORMATION**: The Contractor shall ensure that all Work performed under this Agreement complies with the standards set forth in the Criminal Justice Information Services ("CJIS") Security Policy, attached hereto and incorporated as **Exhibit E**, and all other applicable requirements issued by the Federal Bureau of Investigation ("FBI"). The Contractor is responsible for safeguarding the confidentiality, integrity, and availability of criminal justice information ("CJI") from unauthorized access, use, or disclosure. The Contractor shall assign and maintain internal responsibilities for CJIS compliance and fully cooperate with audits or inspections conducted by the City, the Colorado Bureau of Investigation, or the FBI to verify adherence to the CJIS Security Policy. Any breach or security incident involving CJI must be promptly reported to the City, along with appropriate remedial actions. Contractors with direct or indirect access to CJI shall handle CJI in accordance with the CJIS Security Policy and Title 28 of the Code of Federal Regulations, Part 20. Contractors supporting systems that provide direct access to CJI shall also follow the applicable laws, policies, and manuals incorporated into this Agreement, including but not limited to the NCIC Operating Manual, CCIC Training Manual, Interstate Identification Index / National Fingerprint File Operational and Technical Manual, and Title 28 CFR Part 23. Contractors performing criminal justice functions and accessing CJI shall meet the same training and certification standards as governmental agencies performing comparable duties and shall be subject to audits on the same basis. Prior to receiving access to CJI or Federal Criminal History Record Information ("CHRI"), the Contractor and its personnel shall complete the CJIS Security Addendum certification, attached hereto. The Contractor shall maintain signed certification pages for each individual and provide copies to the City upon request.
17. **GOVERNING LAW; VENUE**: This Agreement will be construed and enforced in accordance with applicable federal law, the laws of the State of Colorado, and the Charter, Revised Municipal Code, ordinances, regulations and Executive Orders of the City and County of Denver, which are expressly incorporated into this Agreement. Unless otherwise specified, any reference to statutes, laws, regulations, charter or code provisions, ordinances, executive orders, or related memoranda, includes amendments or supplements to same. Venue for any legal action relating to this Agreement will be in the District Court of the State of Colorado, Second Judicial District (Denver District Court).
18. **WHEN RIGHTS AND REMEDIES NOT WAIVED**: In no event shall any action by either Party hereunder constitute or be construed to be a waiver by the other Party of any breach of covenant or default which may then exist on the part of the Party alleged to be in breach, and the non-breaching Party's action or inaction when any such breach or default shall exist shall not impair or prejudice any right or remedy available to that Party with respect to such breach or default; and no assent, expressed or implied, to any breach of any

one or more covenants, provisions or conditions of this Agreement shall be deemed or taken to be a waiver of any other breach.

19. **NO THIRD-PARTY BENEFICIARY**: Enforcement of the terms of this Agreement and all rights of action relating to enforcement are strictly reserved to the Parties. Nothing contained in this Agreement gives or allows any claim or right of action to any third person or entity. Any person or entity other than the City or the Contractor receiving services or benefits pursuant to this Agreement is an incidental beneficiary only.
20. **NO AUTHORITY TO BIND CITY TO CONTRACTS**: The Contractor lacks any authority to bind the City on any contractual matters. Final approval of all contractual matters that purport to obligate the City must be executed by the City in accordance with the City's Charter and the Denver Revised Municipal Code.
21. **AGREEMENT AS COMPLETE INTEGRATION-AMENDMENTS**: This Agreement, including its Exhibits and any duly executed Task Orders and amendments, is the complete integration of all understandings between the Parties as to the subject matter of this Agreement. No prior, contemporaneous, or subsequent addition, deletion, or other modification has any force or effect, unless embodied in a written amendment to this Agreement executed by authorized representatives of both Parties. No oral representation by any officer or employee of the City at variance with the terms of this Agreement or any written amendment to this Agreement will have any force or effect or bind the City.
22. **SEVERABILITY**: Except for the provisions of this Agreement requiring appropriation of funds and limiting the total amount payable by the City, if a court of competent jurisdiction finds any provision of this Agreement or any portion of it to be invalid, illegal, or unenforceable, the validity of the remaining portions or provisions will not be affected, if the intent of the Parties can be fulfilled.
23. **CONFLICT OF INTEREST**: No employee of the City shall have any personal or beneficial interest in the Deliverables described in this Agreement. The Contractor shall not hire, or contract for services with, any employee or officer of the City that would be in violation of the City's Code of Ethics, D.R.M.C. § 2-51 et seq., or the Charter §§ 1.2.8, 1.2.9, and 1.2.12. The Contractor shall not engage in any transaction, activity or conduct that would result in a conflict of interest under this Agreement. The Contractor represents that it has disclosed all current or potential conflicts of interest. A conflict of interest shall include transactions, activities or conduct that would affect the judgment, actions or work of the Contractor by placing the Contractor's own interests, or the interests of any party with whom the Contractor has a contractual arrangement, in conflict with those of the City. The City, in its sole discretion, will determine the existence of a conflict of interest and may terminate this Agreement in the event it determines a conflict exists, after it has given the Contractor written notice describing the conflict.
24. **NOTICES**: All notices, demands, requests, or other communications required or permitted under this Agreement shall be in writing and shall be deemed given and effective: (i) immediately upon delivery if sent by email to the email addresses most recently provided by each Party, provided that the sender receives confirmation of delivery or a read receipt; (ii)

one (1) business day after deposit with a nationally recognized overnight courier service; or (iii) three (3) business days after deposit in the United States mail, postage prepaid, certified or registered mail, return receipt requested. All notices to the Contractor shall be sent to the email address most recently provided by the Contractor and to address listed in the caption of this Agreement. All notices to the City shall be sent to the email address most recently provided by the City and to: Chief Information Officer, Denver Technology Services, 201 West Colfax Avenue, Dept. 301, Denver, Colorado 80202; with a copy to: Denver City Attorney's Office, 1437 Bannock St., Room 353, Denver, Colorado 80202. If email delivery fails or is rejected, the sending Party shall promptly send notice by overnight courier or certified mail to the physical addresses specified above. Either Party may update its email address or other contact information by providing written notice to the other Party in accordance with this provision, which change shall be effective upon receipt.

25. **DISPUTES**: The Parties shall attempt to resolve disputes arising out of or relating to this Agreement through the following escalation process before resorting to formal proceedings: (i) the designated representatives of each Party shall meet and confer in good faith to resolve the dispute within fifteen (15) business days of written notice identifying the dispute; (ii) if unresolved, the dispute shall be escalated to the CIO (or designee) and the Contractor's senior executive with authority to bind the Contractor, who shall meet and confer within an additional fifteen (15) business days. If the dispute remains unresolved after exhaustion of this escalation process, either Party may proceed to administrative hearing pursuant to D.R.M.C. § 56-106(b)-(f). For the purposes of that administrative procedure, the City official rendering a final determination shall be the CIO as defined in this Agreement. Nothing in this Section shall prevent either Party from seeking equitable relief as provided in Section 9.6. In the event of a dispute between the Parties, the Contractor will continue to perform its obligations under this Agreement during the resolution of the dispute until this Agreement is terminated in accordance with its terms.
26. **NO DISCRIMINATION IN EMPLOYMENT**: In connection with the performance of Work under this Agreement, the Contractor may not refuse to hire, discharge, promote, demote, or discriminate in matters of compensation against any person otherwise qualified, solely because of race, color, religion, national origin, ethnicity, citizenship, immigration status, gender, age, sexual orientation, gender identity, gender expression, marital status, source of income, military status, protective hairstyle, or disability. The Contractor shall insert the foregoing provision in all subcontracts.
27. **LEGAL AUTHORITY**: The Contractor represents and warrants that it possesses the legal authority, pursuant to any proper, appropriate, and official motion, resolution or action passed or taken, to enter into this Agreement. Each person signing and executing this Agreement on behalf of the Contractor represents and warrants that he has been fully authorized by the Contractor to execute this Agreement on behalf of the Contractor and to validly and legally bind the Contractor to all the terms, performances and provisions of this Agreement. The City shall have the right, in its sole discretion, to either temporarily suspend

or permanently terminate this Agreement if there is a dispute as to the legal authority of either the Contractor or the person signing this Agreement to enter into this Agreement.

28. **LITIGATION REPORTING**: If the Contractor is served with a pleading or other document in connection with an action before a court or other administrative decision making body, and such pleading or document relates to this Agreement or may affect the Contractor's ability to perform its obligations under this Agreement, the Contractor shall, within 10 days after being served, notify the City of such action and deliver copies of such pleading or document, unless protected by law, to the City.
29. **LICENSES, PERMITS, AND OTHER AUTHORIZATIONS**: The Contractor shall secure, prior to the Term, and shall maintain, at its sole expense, all licenses, certifications, rights, permits, and other authorizations required to perform its obligations under this Agreement. This Section is a material part of this Agreement.
30. **NO CONSTRUCTION AGAINST DRAFTING PARTY**: The Parties and their respective counsel have had the opportunity to review this Agreement, and this Agreement will not be construed against any party merely because any provisions of this Agreement were prepared by a particular party.
31. **ORDER OF PRECEDENCE**: In the event of any conflict or inconsistency between the provisions of this Agreement—including the body, Exhibits, attachments, or any Task Orders, invoices, or quotes issued by the Contractor—the following order of precedence shall apply, with higher-ranked documents controlling over lower-ranked documents: first, **Exhibit E** (CJIS Security Addendum); second, the body of this Agreement; third, **Exhibit C** (Information Technology Provisions) and **Exhibit D** (Department of Public Safety Information Technology Provisions); fourth, **Exhibit A** (Statement of Work); fifth, **Exhibit B** (Certificate of Insurance); sixth, **Exhibit F**, Contractor's Master Services and Purchasing Agreement, and finally, duly executed Task Orders, in reverse chronological order. For clarity, no terms contained in any Task Order, invoice, quote, embedded hyperlink, referenced document, or other supplemental material shall be binding on the City or modify the legal, financial, or material terms of this Agreement unless expressly agreed to by both Parties in a written amendment executed by authorized representatives of the Parties. Order Forms and Task Orders may supplement this Agreement solely with respect to specific products, services, quantities, pricing, or delivery terms, and shall not override any other provisions herein. As among Exhibits of equal rank, if a conflict cannot be reconciled through harmonious construction, the provision imposing the greater obligation on the Contractor or the higher standard of security shall govern.

31.1. Scope of Incorporation and Superseded Provisions

31.1.1. **Exhibit F** is incorporated solely for the purpose of identifying the specific devices, services, subscription terms, and technical configurations applicable to the ALPR system procured under this Agreement. **Exhibit F** does not alter, expand, or supersede any legal, financial, or material term of this Agreement. The following **Exhibit F** provisions conflict with this Agreement and are expressly superseded and have no force or effect:

31.1.1.1. § 14.1 (Effect of Termination). The MSRP differential clawback, fee continuity obligation, and device return restriction in **Exhibit F** § 14.1 are superseded in their entirety by § 6 of this Agreement. No early termination fee, MSRP differential, bundled pricing clawback, or penalty of any kind is owed by the City upon any termination of this Agreement, regardless of the basis for termination or the pricing at which devices were procured.

31.1.1.2. § 5 (Returns — All Sales Final). The no-refund policy in **Exhibit F** § 5 does not apply to prepaid subscription or license fees, which are governed solely by § 6.2 of this Agreement.

31.1.1.3. ACEIP Appendix (Customer Experience Improvement Program). The City does not consent to and expressly opts out of the Axon Customer Experience Improvement Program in all forms, including ACEIP Basic and ACEIP Custom. Contractor may not use City Data, Customer Content, or Non-Content Data for product development, AI training, model improvement, or any purpose outside the direct performance of this Agreement. This opt-out is effective as of the Effective Date and does not require a separate email submission by the City.

31.1.1.4. § 12 (IP Rights) and Cloud Services Appendix § 6 (Privacy — Non-Content Data). Axon's IP ownership and data use rights under **Exhibit F** §§ 12 and Cloud Services Appendix § 6 do not extend to City Data, Deliverables, or any work product governed by this Agreement. Axon's right to use Non-Content Data for product development and improvement does not apply to any data that constitutes City Data under this Agreement.

31.1.1.5. § 10 (Design Changes). Axon's right to make unilateral design or feature changes without notice is subordinate to **Exhibit A** and the change management requirements of **Exhibit D**. Any change that materially affects the Specifications or the City's operational use of the ALPR system requires prior written notice to the City and the City's written approval before implementation.

31.1.1.6. ALPR Appendix § 21 (Acceptance Checklist — Deemed Acceptance). The seven-day deemed acceptance provision is modified. The City shall have thirty (30) calendar days following installation completion to review and provide written acceptance of ALPR deliverables. Silence or non-response shall not constitute acceptance.

31.1.1.7. § 3 (Taxes). The City and County of Denver is a tax-exempt municipal entity. **Exhibit F** § 3 is superseded by § 4.5 of this Agreement. Axon shall not invoice the City for sales tax or similar transactional taxes.

31.1.1.8. § 6.2 (Warranty Disclaimer — AS IS). The "AS IS" disclaimer applicable to software and Axon Cloud Services in **Exhibit F** § 6.2 does not apply to any Work, Deliverables, or Services performed under this Agreement, which are governed by §§ 2.2 and 10 hereof. No disclaimer of warranty in **Exhibit F** limits or qualifies the Contractor's indemnification obligations under § 10.1.

31.1.1.9. § 37 (Advertising) / Axon Aid Appendix. Any marketing consent or public announcement authorization contained in **Exhibit F** or its appendices is superseded by § 37 of this Agreement. Axon may not publicly reference the City, this Agreement, or the City's participation in any Axon program without prior written City approval.

32. **SURVIVAL OF CERTAIN PROVISIONS**: The terms of this Agreement, including any Exhibits and attachments, that by reasonable implication contemplate continued performance, rights, or compliance beyond the expiration or termination of this Agreement shall survive such expiration or termination and shall remain enforceable. Without limiting the foregoing, the Contractor's obligations to provide insurance coverage and to indemnify the City shall survive for a period equal to the duration of all applicable statutes of limitation, plus any additional time reasonably necessary to resolve any claims, disputes, or legal proceedings initiated within that period. Any grant of property rights or intellectual property rights to the City that, by its terms, extends beyond the term of this Agreement shall remain in effect after expiration or termination, except in the event of termination due to the City's breach of its payment obligations. Any warranties made available to the City, whether provided under this Agreement or otherwise, shall survive expiration or termination of this Agreement for the full duration specified in the warranty documentation or as permitted by applicable law. Upon expiration or termination of this Agreement, in whole or in part, the Contractor's obligations regarding the return and destruction of City Data shall be governed by **Exhibit C**.

33. **INUREMENT**: The rights and obligations of the Parties herein set forth shall inure to the benefit of and be binding upon the Parties hereto and their respective successors and assigns permitted under this Agreement.

34. **TIME IS OF THE ESSENCE**: The Parties agree that in the performance of the terms, conditions, and requirements of this Agreement, time is of the essence.

35. **FORCE MAJEURE**: Neither Party shall be liable for failure to perform its obligations under this Agreement to the extent such failure results from causes beyond the Party's reasonable control, including war, terrorism, fire, strike, riot, insurrection, natural disaster, epidemic or pandemic, governmental order or regulation, or the complete or partial shutdown of critical infrastructure or manufacturing (each, an "Excusable Delay"). A Party claiming an Excusable Delay shall: (i) notify the other Party in writing within five (5) business days of becoming aware of the event, describing the nature, expected duration, and affected obligations; (ii) use commercially reasonable efforts to mitigate the impact and resume performance as promptly as practicable; and (iii) provide periodic updates on the status of the Excusable Delay. An Excusable Delay shall not excuse the obligation to make payments for Work already performed or accepted. If an Excusable Delay continues for more than ninety (90) consecutive days, the non-delayed Party may terminate this Agreement, or the affected portion thereof, upon thirty (30) days' written notice without liability to the other Party, except for payment for Work satisfactorily completed and accepted prior to termination. For the avoidance of doubt, an Excusable Delay shall not include the

Contractor's inability to hire or retain personnel, financial hardship, or loss of subcontractors.

36. **PARAGRAPH HEADINGS**: The captions and headings set forth herein are for convenience of reference only and shall not be construed to define or limit the terms and provisions hereof.
37. **ADVERTISING AND PUBLIC DISCLOSURE**: The Contractor shall not include any reference to this Agreement or to Work performed pursuant to this Agreement in any of the Contractor's advertising or public relations materials without first obtaining the City' written approval. Any oral presentation or written materials related to Work performed under this Agreement will be limited to Deliverables that have been accepted by the City. The Contractor shall notify the City in advance of the date and time of any presentation. Nothing in this provision precludes the transmittal of any information to City officials.
38. **EXTERNAL TERMS AND CONDITIONS DISCLAIMER**: Notwithstanding anything to the contrary herein, the City shall not be subject to any provision including any terms, conditions, or agreements, and links thereto, appearing on the Contractor's or a Subcontractor's website, forms, or any provision incorporated into any click-through or online agreements related to the Work unless that provision is specifically incorporated into this Agreement.
39. **PROHIBITED TERMS**: Any term included in this Agreement that requires the City to indemnify or hold the Contractor harmless; requires the City to agree to binding arbitration; limits the Contractor's liability for damages resulting from death, bodily injury, or damage to tangible property; requires payment for any obligation where there has not been an appropriation; requires venue and jurisdiction outside of the Colorado; or seeks to modify the order of precedence, as stated in the main body of this Agreement; or that conflicts with this provision in any way shall be void ab initio. Except as otherwise provided for certain intergovernmental agreements, all contracts entered into by the City shall be governed by the laws of the State of Colorado, regardless of any conflicting provision or choice-of-law term contained therein.
40. **USE, POSSESSION OR SALE OF ALCOHOL OR DRUGS**: To the extent applicable, the Contractor shall cooperate and comply with the provisions of Executive Order 94 and Attachment A thereto concerning the use, possession or sale of alcohol or drugs. Violation of these provisions or refusal to cooperate with implementation of the policy can result in the City barring the Contractor from City facilities or participating in City operations.
41. **CITY EXECUTION OF AGREEMENT**: This Agreement is expressly subject to and shall not be or become effective or binding on the City until it has been fully executed by all signatories of the City and County of Denver.
42. **COUNTERPARTS OF THIS AGREEMENT**: This Agreement may be executed in counterparts, each of which shall be deemed to be an original of this Agreement.
43. **ELECTRONIC SIGNATURES AND ELECTRONIC RECORDS**: The Contractor consents to the use of electronic signatures by the City. This Agreement, and any other documents requiring a signature hereunder, may be signed electronically by the City in the

manner specified by the City. The Parties agree not to deny the legal effect or enforceability of this Agreement solely because it is in electronic form or because an electronic record was used in its formation. The Parties agree not to object to the admissibility of this Agreement in the form of an electronic record, or a paper copy of an electronic document, or a paper copy of a document bearing an electronic signature, on the ground that it is an electronic record or electronic signature or that it is not in its original form or is not an original.

44. **ATTACHED EXHIBITS INCORPORATED**: The following attached exhibits are hereby incorporated into and made a material part of this Agreement: **Exhibit A**, Statement of Work and Quote Q-801736-46091LJ; **Exhibit B**, Certificate of Insurance; **Exhibit C**, Information Technology Provisions; **Exhibit D**, Department of Public Safety Information Technology Provisions; **Exhibit E**, Criminal Justice Information Services Security Addendum; and **Exhibit F,** Contractor's Master Services and Purchasing Agreement.

REMAINDER OF PAGE INTENTIONALLY LEFT BLANK

Contract Control Number: POLIC-202683606-00
Contractor Name: AXON ENTERPRISE INC

IN WITNESS WHEREOF, the parties have set their hands and affixed their seals at Denver, Colorado as of:

SEAL

CITY AND COUNTY OF DENVER:

ATTEST:

By: _____

_____

APPROVED AS TO FORM:

Attorney for the City and County of Denver

By: _____

REGISTERED AND COUNTERSIGNED:

By: _____

By: _____

Contract Control Number: POLIC-202683606-00
Contractor Name: AXON ENTERPRISE INC

By: Signed by: Robert Driscoll 55DAEBB131A4424...

Name: Robert Driscoll
(please print)

Title: VP, Deputy General Counsel
(please print)

ATTEST: [if required]

By: _____

Name: _____
(please print)

Title: _____
(please print)

Axon Enterprise, Inc.
17800 N 85th St
Scottsdale, Arizona 85255
United States
VAT: 86-0741227
Domestic:(800) 978-2737
International: +1.800.978.2737

EXHIBIT A

Q-801736-46091LJ

Issued: 03/10/2026

Quote Expiration:

Estimated Contract Start Date: 06/01/2026

Account Number: 108689

Payment Terms: N30

Mode of Delivery: AUTO-GND

Credit/Debit Amount: $0.00

SHIP TO	BILL TO
Denver Police Department - CO 1331 Cherokee St Denver, CO 80204-2720 USA	Denver Police Department - CO PO Box 40098 Denver CO 80204-0098 USA Email:

SALES REPRESENTATIVE	PRIMARY CONTACT
Ben Rubke Phone: +1 4153149573 Email: brubke@axon.com Fax:	Cliff Barnes Phone: (720) 468-0811 Email: clifford.barnes@denvergov.org Fax:

Quote Summary

Program Length	12 Months
TOTAL COST	$149,999.00
ESTIMATED TOTAL W/ TAX	$149,999.00

Discount Summary

Average Savings Per Year	$279,951.00
TOTAL SAVINGS	$279,951.00

Payment Summary

Date	Subtotal	Tax	Total
May 2026	$149,999.00	$0.00	$149,999.00
Total	**$149,999.00**	**$0.00**	**$149,999.00**

Quote Unbundled Price:	**$429,950.00**
Quote List Price:	**$429,950.00**
Quote Subtotal:	**$149,999.00**

Pricing

All deliverables are detailed in Delivery Schedules section lower in proposal

Item	Description	Qty	Term	Unbundled	List Price	Net Price	Subtotal	Tax	Total
A la Carte Hardware									
102538	AXON OUTPOST - TOP MOUNT END CAP - STANDARD	50			$100.00	$50.00	$2,500.00	$0.00	$2,500.00
102488	AXON OUTPOST - SOLAR PANEL - 100W	50			$145.00	$50.00	$2,500.00	$0.00	$2,500.00
102543	AXON OUTPOST - BATTERY & CHARGER ENCLOSURE - EXTENDED	50			$950.00	$100.00	$5,000.00	$0.00	$5,000.00
102737	AXON OUTPOST - STANDARD SOLAR HARDWARE KIT	50			$400.00	$199.98	$9,999.00	$0.00	$9,999.00
102032	AXON OUTPOST - CAMERA	50			$1,250.00	$200.00	$10,000.00	$0.00	$10,000.00
102552	AXON OUTPOST - POLE - STANDARD	50			$1,495.00	$200.00	$10,000.00	$0.00	$10,000.00
A la Carte Software									
102142	AXON VEHICLE INTELLIGENCE - ALPR LICENSE	50	12		$182.00	$166.67	$100,000.00	$0.00	$100,000.00
A la Carte Services									
102136	AXON OUTPOST - STANDARD INSTALLATION	50			$875.00	$200.00	$10,000.00	$0.00	$10,000.00
A la Carte Warranties									
102703	AXON OUTPOST - WARRANTY - VANDALISM/ACCIDENT EXTENSION	50	1		$1,200.00	$0.00	$0.00	$0.00	$0.00
Total							**$149,999.00**	**$0.00**	**$149,999.00**

Delivery Schedule

Hardware

Bundle	Item	Description	QTY	Shipping Location	Estimated Delivery Date
A la Carte	102032	AXON OUTPOST - CAMERA	50	1	05/01/2026
A la Carte	102488	AXON OUTPOST - SOLAR PANEL - 100W	50	1	05/01/2026
A la Carte	102538	AXON OUTPOST - TOP MOUNT END CAP - STANDARD	50	1	05/01/2026
A la Carte	102543	AXON OUTPOST - BATTERY & CHARGER ENCLOSURE - EXTENDED	50	1	05/01/2026
A la Carte	102552	AXON OUTPOST - POLE - STANDARD	50	1	05/01/2026
A la Carte	102737	AXON OUTPOST - STANDARD SOLAR HARDWARE KIT	50	1	05/01/2026

Software

Bundle	Item	Description	QTY	Estimated Start Date	Estimated End Date
A la Carte	102142	AXON VEHICLE INTELLIGENCE - ALPR LICENSE	50	06/01/2026	05/31/2027

Services

Services

Bundle	Item	Description	QTY
A la Carte	102136	AXON OUTPOST - STANDARD INSTALLATION	50

Warranties

Bundle	Item	Description	QTY	Estimated Start Date	Estimated End Date
A la Carte	102703	AXON OUTPOST - WARRANTY - VANDALISM/ACCIDENT EXTENSION	50	05/01/2027	05/31/2027

Shipping Locations

Location Number	Street	City	State	Zip	Country
1	1331 Cherokee St	Denver	CO	80204-2720	USA

Payment Details

May 2026

Invoice Plan	Item	Description	Qty	Subtotal	Tax Total	
Upfront	102032	AXON OUTPOST - CAMERA	50	$10,000.00	$0.00	$10,000.00
Upfront	102136	AXON OUTPOST - STANDARD INSTALLATION	50	$10,000.00	$0.00	$10,000.00
Upfront	102142	AXON VEHICLE INTELLIGENCE - ALPR LICENSE	50	$100,000.00	$0.00	$100,000.00
Upfront	102488	AXON OUTPOST - SOLAR PANEL - 100W	50	$2,500.00	$0.00	$2,500.00
Upfront	102538	AXON OUTPOST - TOP MOUNT END CAP - STANDARD	50	$2,500.00	$0.00	$2,500.00
Upfront	102543	AXON OUTPOST - BATTERY & CHARGER ENCLOSURE - EXTENDED	50	$5,000.00	$0.00	$5,000.00
Upfront	102552	AXON OUTPOST - POLE - STANDARD	50	$10,000.00	$0.00	$10,000.00
Upfront	102737	AXON OUTPOST - STANDARD SOLAR HARDWARE KIT	50	$9,999.00	$0.00	$9,999.00
Invoice Upon Fulfillment	102703	AXON OUTPOST - WARRANTY - VANDALISM/ACCIDENT EXTENSION	50	$0.00	$0.00	$0.00
Total				**$149,999.00**	**$0.00**	**$149,999.00**

Tax is estimated based on rates applicable at date of quote and subject to change at time of invoicing. If a tax exemption certificate should be applied, please submit prior to invoicing.

Standard Terms and Conditions

Axon Enterprise Inc. Sales Terms and Conditions

Acceptance of Terms:

Any purchase order issued in response to this Quote is subject solely to the terms and conditions attached to this Quote.

Exceptions to Standard Terms and Conditions

Rewrite Estimates

Estimated Amounts and Contract Terminations. Any amounts stated as due under existing or terminated contracts — including contract transfer balances carried forward to new or pending contracts — are estimates based on payments received as of the calculation date. These estimates may be adjusted if new contracts are not executed on the anticipated dates or if expected payments are not made.

Refresh Shipment Timing

Technology Assurance Plan (TAP) Refresh Prior to Renewal. For Customers with expiring agreements that include TAP refresh rights, Axon may, in its discretion, ship refresh hardware under the existing contract while renewal or replacement agreements are in progress. Any such shipments will be deemed made under the terms of the existing contract until the new contract is fully executed, after which any applicable updates, fees, or adjustments will apply.

Shipment Timing

Shipment Variance. Estimated shipment dates are provided for planning purposes only and are not guarantees. Axon may ship hardware before or after the estimated shipment date, and failure to meet an estimated shipment date will not, by itself, constitute a breach, provided Axon uses commercially reasonable efforts to meet estimated shipment dates.

EXHIBIT B

ACORD®

CERTIFICATE OF LIABILITY INSURANCE

DATE(MM/DD/YYYY)
08/12/2025

THIS CERTIFICATE IS ISSUED AS A MATTER OF INFORMATION ONLY AND CONFERS NO RIGHTS UPON THE CERTIFICATE HOLDER. THIS CERTIFICATE DOES NOT AFFIRMATIVELY OR NEGATIVELY AMEND, EXTEND OR ALTER THE COVERAGE AFFORDED BY THE POLICIES BELOW. THIS CERTIFICATE OF INSURANCE DOES NOT CONSTITUTE A CONTRACT BETWEEN THE ISSUING INSURER(S), AUTHORIZED REPRESENTATIVE OR PRODUCER, AND THE CERTIFICATE HOLDER.

IMPORTANT: If the certificate holder is an ADDITIONAL INSURED, the policy(ies) must have ADDITIONAL INSURED provisions or be endorsed. If SUBROGATION IS WAIVED, subject to the terms and conditions of the policy, certain policies may require an endorsement. A statement on this certificate does not confer rights to the certificate holder in lieu of such endorsement(s).

PRODUCER
Aon Risk Insurance Services West, Inc.
Phoenix AZ Office
4300 East Camelback Rd.
Suite 460
Phoenix AZ 85018 USA

CONTACT NAME:
PHONE (A/C. No. Ext): 8662837122 **FAX (A/C. No.):** (800) 363-0105
E-MAIL ADDRESS:

INSURER(S) AFFORDING COVERAGE		NAIC #
INSURER A:	National Casualty Company	11991
INSURER B:	Scottsdale Ins Company	41297
INSURER C:		
INSURER D:		
INSURER E:		
INSURER F:		

INSURED
Axon Enterprise, Inc.
17800 N. 85th Street
Scottsdale AZ 85255 USA

COVERAGES **CERTIFICATE NUMBER:** 570114905955 **REVISION NUMBER:**

THIS IS TO CERTIFY THAT THE POLICIES OF INSURANCE LISTED BELOW HAVE BEEN ISSUED TO THE INSURED NAMED ABOVE FOR THE POLICY PERIOD INDICATED. NOTWITHSTANDING ANY REQUIREMENT, TERM OR CONDITION OF ANY CONTRACT OR OTHER DOCUMENT WITH RESPECT TO WHICH THIS CERTIFICATE MAY BE ISSUED OR MAY PERTAIN, THE INSURANCE AFFORDED BY THE POLICIES DESCRIBED HEREIN IS SUBJECT TO ALL THE TERMS, EXCLUSIONS AND CONDITIONS OF SUCH POLICIES. LIMITS SHOWN MAY HAVE BEEN REDUCED BY PAID CLAIMS.

Limits shown are as requested

INSR LTR	TYPE OF INSURANCE	ADDL INSD	SUBR WVD	POLICY NUMBER	POLICY EFF (MM/DD/YYYY)	POLICY EXP (MM/DD/YYYY)	LIMITS	
A	X **COMMERCIAL GENERAL LIABILITY** CLAIMS-MADE / X OCCUR X see Prod Liab info att'd GEN'L AGGREGATE LIMIT APPLIES PER: POLICY / X PRO-JECT / LOC OTHER: Xcl Prod/Comp Ops	Y	Y	NGO0001949 SIR applies per policy terms & conditions	08/08/2025	08/01/2026	EACH OCCURRENCE DAMAGE TO RENTED PREMISES (Ea occurrence) MED EXP (Any one person) PERSONAL & ADV INJURY GENERAL AGGREGATE PRODUCTS - COMP/OP AGG	$2,000,000 $1,000,000 $50,000 $2,000,000 $4,000,000 Excluded
A	**AUTOMOBILE LIABILITY** X ANY AUTO OWNED AUTOS ONLY / SCHEDULED AUTOS HIRED AUTOS ONLY / NON-OWNED AUTOS ONLY	Y	Y	NGO0001948	08/08/2025	08/01/2026	COMBINED SINGLE LIMIT (Ea accident) BODILY INJURY (Per person) BODILY INJURY (Per accident) PROPERTY DAMAGE (Per accident)	$1,000,000
B	X **UMBRELLA LIAB** / X OCCUR **EXCESS LIAB** / CLAIMS-MADE DED / X RETENTION $10,000	Y	Y	UNS0000106	08/08/2025	08/01/2026	EACH OCCURRENCE AGGREGATE	$10,000,000 $10,000,000
A	**WORKERS COMPENSATION AND EMPLOYERS' LIABILITY** ANY PROPRIETOR / PARTNER / EXECUTIVE OFFICER/MEMBER EXCLUDED? Y/N: N **(Mandatory in NH)** If yes, describe under DESCRIPTION OF OPERATIONS below	N / A	Y	WCC600103A	08/08/2025	08/08/2026	X PER STATUTE / OTH-ER E.L. EACH ACCIDENT E.L. DISEASE-EA EMPLOYEE E.L. DISEASE-POLICY LIMIT	 $1,000,000 $1,000,000 $1,000,000

DESCRIPTION OF OPERATIONS / LOCATIONS / VEHICLES (ACORD 101, Additional Remarks Schedule, may be attached if more space is required)

Certificate Holder is included as Additional Insured in accordance with the policy provisions of the Automobile Liability, Excess Liability and General Liability policies. Automobile Liability, Excess Liability and General Liability policies evidenced herein is Primary to other insurance available to an Additional Insured, but only in accordance with the policy's provisions. Automobile Liability, Excess Liability and General Liability policies evidenced herein is Non-Contributory to other insurance available to an Additional Insured, but only in accordance with the policy's provisions. A Waiver of Subrogation is granted in favor of Certificate Holder in accordance with the policy provisions of the Automobile Liability, Excess Liability, General Liability and Workers Compensation policies.

CERTIFICATE HOLDER

City and County of Denver
201 W. Colfax Ave.
Denver CO 80202 USA

CANCELLATION

SHOULD ANY OF THE ABOVE DESCRIBED POLICIES BE CANCELLED BEFORE THE EXPIRATION DATE THEREOF, NOTICE WILL BE DELIVERED IN ACCORDANCE WITH THE POLICY PROVISIONS.

AUTHORIZED REPRESENTATIVE

Aon Risk Insurance Services West, Inc.

Holder Identifier :

Certificate No : 570114905955

AGENCY CUSTOMER ID: 570000007117

LOC #:

ADDITIONAL REMARKS SCHEDULE

AGENCY		NAMED INSURED
Aon Risk Insurance Services West, Inc.		Axon Enterprise, Inc.
POLICY NUMBER		
See Certificate Number: 570114905955		
CARRIER	NAIC CODE	EFFECTIVE DATE:
See Certificate Number: 570114905955		

ADDITIONAL REMARKS

THIS ADDITIONAL REMARKS FORM IS A SCHEDULE TO ACORD FORM,

FORM NUMBER: ACORD 25 **FORM TITLE:** Certificate of Liability Insurance

Products Liability Schedule

Products/Completed Operations Coverage
8/8/2025-8/1/2026:

Policy #034064091
Lexington Insurance Company
Claims Made Coverage Form - Products Liability
$15,000,000 Each Occurrence Limit
$15,000,000 Products/Completed Operations Aggregate Limit
$ 5,000,000 Per Occurrence Self Insured Retention

Policy #034064092
Lexington Insurance Company
Occurrence Coverage Form - Products Liability
$15,000,000 Each Occurrence Limit
$15,000,000 Products/Completed Operations Aggregate Limit
$ 5,000,000 Per Occurrence Self Insured Retention

CERTIFICATE OF LIABILITY INSURANCE

DATE(MM/DD/YYYY)
08/05/2025

THIS CERTIFICATE IS ISSUED AS A MATTER OF INFORMATION ONLY AND CONFERS NO RIGHTS UPON THE CERTIFICATE HOLDER. THIS CERTIFICATE DOES NOT AFFIRMATIVELY OR NEGATIVELY AMEND, EXTEND OR ALTER THE COVERAGE AFFORDED BY THE POLICIES BELOW. THIS CERTIFICATE OF INSURANCE DOES NOT CONSTITUTE A CONTRACT BETWEEN THE ISSUING INSURER(S), AUTHORIZED REPRESENTATIVE OR PRODUCER, AND THE CERTIFICATE HOLDER.

IMPORTANT: If the certificate holder is an ADDITIONAL INSURED, the policy(ies) must have ADDITIONAL INSURED provisions or be endorsed. If SUBROGATION IS WAIVED, subject to the terms and conditions of the policy, certain policies may require an endorsement. A statement on this certificate does not confer rights to the certificate holder in lieu of such endorsement(s).

PRODUCER Aon Risk Insurance Services West, Inc. Phoenix AZ Office 4300 East Camelback Rd. Suite 460 Phoenix AZ 85018 USA	CONTACT NAME: PHONE (A/C. No. Ext): (866) 283-7122 FAX (A/C. No.): (800) 363-0105 E-MAIL ADDRESS:
INSURED Axon Enterprise, Inc. 17800 N. 85th Street Scottsdale AZ 85255 USA	INSURER(S) AFFORDING COVERAGE — NAIC # INSURER A: AIG Specialty Insurance Company — 26883 INSURER B: INSURER C: INSURER D: INSURER E: INSURER F:

Holder Identifier :

COVERAGES **CERTIFICATE NUMBER:** 570114821017 **REVISION NUMBER:**

THIS IS TO CERTIFY THAT THE POLICIES OF INSURANCE LISTED BELOW HAVE BEEN ISSUED TO THE INSURED NAMED ABOVE FOR THE POLICY PERIOD INDICATED. NOTWITHSTANDING ANY REQUIREMENT, TERM OR CONDITION OF ANY CONTRACT OR OTHER DOCUMENT WITH RESPECT TO WHICH THIS CERTIFICATE MAY BE ISSUED OR MAY PERTAIN, THE INSURANCE AFFORDED BY THE POLICIES DESCRIBED HEREIN IS SUBJECT TO ALL THE TERMS, EXCLUSIONS AND CONDITIONS OF SUCH POLICIES. LIMITS SHOWN MAY HAVE BEEN REDUCED BY PAID CLAIMS. Limits shown are as requested

INSR LTR	TYPE OF INSURANCE	ADDL INSD	SUBR WVD	POLICY NUMBER	POLICY EFF (MM/DD/YYYY)	POLICY EXP (MM/DD/YYYY)	LIMITS	
	COMMERCIAL GENERAL LIABILITY						EACH OCCURRENCE	
	☐ CLAIMS-MADE ☐ OCCUR						DAMAGE TO RENTED PREMISES (Ea occurrence)	
							MED EXP (Any one person)	
	GEN'L AGGREGATE LIMIT APPLIES PER:						PERSONAL & ADV INJURY	
	☐ POLICY ☐ PRO-JECT ☐ LOC						GENERAL AGGREGATE	
	☐ OTHER:						PRODUCTS - COMP/OP AGG	
	AUTOMOBILE LIABILITY						COMBINED SINGLE LIMIT (Ea accident)	
	☐ ANY AUTO						BODILY INJURY (Per person)	
	☐ OWNED AUTOS ONLY ☐ SCHEDULED AUTOS						BODILY INJURY (Per accident)	
	☐ HIRED AUTOS ONLY ☐ NON-OWNED AUTOS ONLY						PROPERTY DAMAGE (Per accident)	
	☐ UMBRELLA LIAB ☐ OCCUR						EACH OCCURRENCE	
	☐ EXCESS LIAB ☐ CLAIMS-MADE						AGGREGATE	
	☐ DED ☐ RETENTION							
	WORKERS COMPENSATION AND EMPLOYERS' LIABILITY Y / N						☐ PER STATUTE ☐ OTH-ER	
	ANY PROPRIETOR / PARTNER / EXECUTIVE OFFICER/MEMBER EXCLUDED? ☐ N / A						E.L. EACH ACCIDENT	
	(Mandatory in NH) If yes, describe under DESCRIPTION OF OPERATIONS below						E.L. DISEASE-EA EMPLOYEE	
							E.L. DISEASE-POLICY LIMIT	
A	E&O - Technology			023593127 Cyber/Tech E&O SIR applies per policy terms & conditions	08/01/2025	08/01/2026	Security/Privacy Li Policy Limit SIR	$5,000,000 $5,000,000 $1,000,000

Certificate No : 570114821017

DESCRIPTION OF OPERATIONS / LOCATIONS / VEHICLES (ACORD 101, Additional Remarks Schedule, may be attached if more space is required)

RE: Body Cameras, Accessories, Equipment. The City and County of Denver, its elected, appointed officials, employees and volunteers are included as Additional Insured in accordance with the policy provisions of the Cyber Liability Policy. A Waiver of Subrogation is granted in favor of Certificate Holder in accordance with the policy provisions of the Cyber Liability policy.

CERTIFICATE HOLDER

City & County of Denver
Manager of Safety,
1331 Cherokee Street, Room 302
Denver CO 80202 USA

CANCELLATION

SHOULD ANY OF THE ABOVE DESCRIBED POLICIES BE CANCELLED BEFORE THE EXPIRATION DATE THEREOF, NOTICE WILL BE DELIVERED IN ACCORDANCE WITH THE POLICY PROVISIONS.

AUTHORIZED REPRESENTATIVE

Aon Risk Insurance Services West Inc.

EXHIBIT C, INFORMATION TECHNOLOGY PROVISIONS

This Exhibit regarding Information Technology Provisions (this "Exhibit") is a material part of the Agreement between the Parties to which this Exhibit is attached. In addition to the requirements of the main body of this Agreement, the Contractor shall protect the City's information technology resources and City Data in accordance with this Exhibit. All provisions of this Exhibit that refer to the Contractor shall apply equally to any Subcontractor performing work in connection with this Agreement. Unless the context clearly requires a distinction between the Agreement and this Exhibit, all references to "Agreement" shall include this Exhibit. Capitalized terms used but not defined in this Exhibit have the meanings assigned to them in the Framework Agreement.

1. TECHNOLOGY SERVICES SPECIFICATIONS

1.1. Identity and Access Management

1.1.1. User ID Credentials: Internal corporate or customer (tenant) user account credentials shall be restricted, ensuring appropriate identity, entitlement, and access management and in accordance with established policies and procedures, as follows:

1.1.1.1. Identity trust verification and service-to-service application (API) and information processing interoperability (e.g., SSO and Federation);

1.1.1.2. Account credential lifecycle management from instantiation through revocation;

1.1.1.3. Account credential and/or identity store minimization or re-use when feasible; and

1.1.1.4. Adherence to industry acceptable and/or regulatory compliant authentication, authorization, and accounting (AAA) rules (e.g., strong/multi-factor, expirable, non-shared authentication secrets).

1.1.2. IdM Integration: The City's Identity and Access Management ("IdM") system is an integrated infrastructure solution that enables many of the City's services and online resources to operate more efficiently, effectively, and securely. All new and proposed applications must utilize the authentication and authorization functions and components of IdM. Strong authentication is required for privileged accounts or accounts with access to sensitive information. This technical requirement applies to all solutions regardless of where the application is hosted.

1.2. Software Updates and Maintenance

1.2.1. Updates & Upgrades: During the Term, the Contractor shall provide the City with all updates and upgrades to the On-Premise Software and SaaS without additional charge, consistent with what the Contractor provides to its customers generally. Upon delivery, upgrades become part of the licensed software and are subject to all terms of this Agreement.

1.2.2. Compatibility with Third-Party Software: The Contractor shall ensure that its Work remains compatible with current, generally available versions of any third-

party software necessary for the Work to function as intended. The Contractor shall complete any necessary updates to maintain such compatibility within a commercially reasonable timeframe following new releases of such third-party software. If the Contractor's Work becomes incompatible with current third-party software versions, the City may, in its discretion, suspend use of the incompatible Work without penalty until compatibility is restored. The Contractor shall bear all costs of maintaining third-party software compatibility.

1.2.3. Supported Releases: The Contractor shall maintain all third-party software used in the development, execution, or delivery of the Work on vendor-supported releases throughout the Term, including all code libraries, frameworks, components, and other products, whether commercial, open-source, or closed-source. This requirement extends to any Contractor-controlled systems operating on the City's network, including applications, firewalls, and physical or virtual appliances. The Contractor shall not require the City to use end-of-life or unsupported software versions to maintain compatibility with the Contractor's Work.

1.3. License and Fee Management

1.3.1. Adjustment of Licenses: The City may increase or decrease the number of licenses at each anniversary date by providing written notice to the Contractor at least sixty (60) days prior. The Contractor shall adjust invoicing accordingly based on the unit price per license specified in this Agreement.

1.3.2. Fee Accrual: Notwithstanding any provision to the contrary, fees for maintenance, support, SaaS subscriptions, or similar ongoing services shall not accrue, and no subscription periods shall commence, before the City's Acceptance or first production use of the Work, whichever occurs first. For purposes of this Section, "first production use" does not include any pilot, beta, trial, testing, or sandbox deployment.

2. DATA GOVERNANCE AND OWNERSHIP

2.1. Data Ownership and Usage Rights: Unless otherwise required by law, the City has exclusive ownership of all City Data, including all City Data created, processed, or derived in connection with this Agreement. The Parties recognize and agree that the Contractor is a bailee for hire with respect to City Data. The Contractor's possession and use of City Data is solely on the City's behalf and limited to performing its obligations under this Agreement. The City retains the right to access and retrieve City Data at any time during the Term. This Agreement grants neither Party any rights to the other Party's data, content, or intellectual property except as expressly stated herein.

2.2. Data Use Restrictions: The Contractor shall not use City Data for any purpose other than performing its obligations under this Agreement, except as expressly authorized in writing by the City or as required by applicable law. There will be no shared network use of City Data and any sharing of such data remains exclusively within the discretion and control of the City. Prohibited activities further include, without limitation: (i) Data mining, analysis, or processing of City Data for any purpose other

than performing the Contractor's obligations under this Agreement; and (ii) Sharing, selling, licensing, or otherwise disclosing City Data to third parties for purposes unrelated to this Agreement.

2.3. **Artificial Intelligence Systems**: The Contractor shall not use City Data to train, improve, or develop any artificial intelligence, machine learning models, algorithms, or automated decision-making systems without express written authorization from the City. If the Work involves use of any high-risk artificial intelligence system as defined in Colo. Rev. Stat. § 6-1-1701(9), the Contractor shall comply with all requirements of Colo. Rev. Stat. § 6-1-1701 et seq., including exercising reasonable care to protect against algorithmic discrimination and ensuring appropriate human oversight, documentation, and transparency for consequential decisions.

2.4. **Data Lifecycle Management**

2.4.1. **Backup and Preservation**: The Contractor shall maintain regular backups of all City Data using industry-standard procedures and security measures. The Contractor shall preserve City Data for litigation holds as requested by the City and shall not obstruct the City's ability to access or retrieve City Data stored by the Contractor.

2.4.2. **Retention and Destruction**: The Contractor shall retain City Data only as long as necessary to perform its obligations under this Agreement or as required by law. Upon expiration or termination of this Agreement, the Contractor shall, as directed by the City, either (i) make City Data available to the City for retrieval, or (ii) securely destroy all City Data and certify such destruction in writing. Destruction shall render City Data permanently unreadable and indecipherable through shredding, erasing, secure wiping, or other methods approved by the City. These obligations apply equally to the Contractor's successors, including any trustee in bankruptcy, and survive termination of this Agreement.

2.5. **Data Location Requirements**: All City Data must be stored, processed, and transmitted solely within the United States unless the City provides express written approval specifying permitted locations, duration, security requirements, and conditions for any exception. Notwithstanding anything to the contrary in this Agreement, the City has no responsibility or obligation to comply with foreign data protection laws or policies, including but not limited to the General Data Protection Regulation of the European Union.

2.6. **Monitoring, Audit, and Survivability**: The City may inspect and monitor the Contractor's access to and use of City Data and evaluate the Contractor's data protection controls, subject to reasonable advance notice and the Contractor's reasonable security requirements. The data governance and protection obligations in this Section survive termination or expiration of this Agreement and remain in effect until all City Data is properly returned, securely destroyed, or as otherwise required by law.

2.7. **Mandatory Regulatory Disclosures**: The Contractor shall promptly provide the City with a copy of any disclosure the Contractor is required to file with any regulatory

body as a result of a Security Breach or other incident arising from or related to this Agreement, including disclosures mandated by the Securities and Exchange Commission or any state or federal regulatory authority. If the contents of such disclosure are protected by law, the Contractor shall instead provide the City with prompt written notice that a disclosure was required, identifying the regulatory body to which the disclosure was made and the general nature of the incident giving rise to the disclosure obligation.

3. SECURITY STANDARDS AND SAFEGUARDS

3.1. **Mandatory Security Standards**: When maintaining, storing, or processing PII on the City's behalf, the Contractor is a "Third-Party Service Provider" under Colo. Rev. Stat. § 24-73-103(1)(i) and shall maintain security procedures consistent with Colo. Rev. Stat. § 24-73-101 et seq. The Contractor shall implement and maintain security safeguards appropriate to the sensitivity and volume of City Data, using controls and practices consistent with applicable industry standards and legal requirements. These safeguards must protect City Data from unauthorized access, use, modification, disclosure, or destruction.

3.2. **Encryption Requirements**: All City Data must be encrypted both in transit and at rest using National Institute of Standards and Technology (NIST) approved encryption methods and standards. This requirement applies to all file transfers, transmissions, web interfaces, storage systems, and backups containing City Data.

3.3. **Software Security and Vulnerability Management**: The Contractor shall not use software with known security vulnerabilities in connection with City services. The Contractor shall regularly consult the Cybersecurity and Infrastructure Security Agency (CISA) Known Exploited Vulnerabilities Catalog and other authoritative vulnerability databases and shall promptly remediate any applicable vulnerabilities identified therein. The Contractor shall maintain a documented vulnerability management program and provide evidence of compliance upon the City's request. Upon request, the Contractor shall meet with City to discuss and provide and review a software bill of materials ("SBOM") annually or upon major changes to the solution(s) provided to the City under this Agreement.

3.4. **Software Licensing and Intellectual Property Compliance**: The Contractor shall use only properly licensed software and technology in all systems that access, process, store, or transmit City Data. The Contractor shall maintain compliance with all applicable intellectual property requirements, including copyright laws and software license terms, for all software and technology deployed under this Agreement. The Contractor shall provide proof of licensing compliance upon the City's request.

3.5. **Network Security Controls**: The Contractor shall implement network security measures appropriate to the sensitivity of accessible City Data, including but not limited to firewalls, intrusion detection and prevention systems, security monitoring, and network segmentation. The Contractor shall conduct periodic security assessments and penetration testing in accordance with this Exhibit and shall remediate identified vulnerabilities according to industry-standard timelines based on severity.

4. PERSONNEL SECURITY AND ACCESS CONTROLS

4.1. Personnel Access and Qualifications: The Contractor shall grant access to City Data only to personnel who require such access to perform their assigned responsibilities under this Agreement. Before granting access to City Data, the Contractor shall ensure such personnel have: (i) Completed background screenings appropriate to the sensitivity of accessible City Data and consistent with applicable law; (ii) Received training on data protection requirements applicable to this Agreement; and (iii) Acknowledged in writing their obligations to protect City Data. The Contractor shall promptly revoke access when personnel no longer require it or upon termination of their employment or engagement. If the Contractor has access to Federal Tax Information ("FTI") under this Agreement, the Contractor shall comply with the background check and safeguarding requirements of IRS Publication 1075.

4.2. Access Control Requirements: The Contractor shall implement and maintain access controls for all personnel with access to City Data, including: (i) Least Privilege Access: Limiting access rights to the minimum necessary to perform assigned duties; (ii) Multi-Factor Authentication: Requiring multi-factor authentication for all systems that access, process, store, or transmit City Data; (iii) Access Logging and Monitoring: Maintaining logs of all access to City Data, including user identity, date, time, and nature of access. Logs shall be retained for at least one (1) year and made available to the City upon request; and (iv) Periodic Access Reviews: Conducting regular reviews to ensure access rights remain appropriate and removing access immediately upon termination of employment or change in role.

4.3. Confidentiality Obligations: The Contractor shall require all personnel with access to City Data to execute nondisclosure agreements that are at least as protective of City Data as the confidentiality terms of this Agreement. The Contractor remains fully responsible for all acts and omissions regarding City Data by its personnel, regardless of whether such personnel have executed nondisclosure agreements. Upon the City's request, the Contractor shall provide copies of executed nondisclosure agreements with Subcontractors and other third parties who have access to City Data under this Agreement.

5. SECURITY AUDITS AND TESTING

5.1. Baseline Audit Requirements

5.1.1. The Contractor shall conduct or have conducted the following security assessments at its own expense:

5.1.1.1. Annual Security Audit: Initially prior to the Effective Date, and at least annually thereafter, an SSAE 18 SOC 2 Type 2 audit (or successor standard) of the Contractor's security policies, procedures, and controls applicable to the Work performed under this Agreement. The Contractor shall provide audit results to the City within seven (7) business days of receipt;

5.1.1.2. Vulnerability Scanning: At least quarterly, external and internal vulnerability scans of systems and facilities used to deliver the Work, including

public-facing websites. Scans shall identify vulnerabilities by severity (critical, high, medium, low);

5.1.1.3. **Penetration Testing**: At least annually, a formal penetration test performed by qualified personnel of systems and facilities used to deliver the Work; and

5.1.1.4. **Data Integrity Audits**: At least annually, third-party verification of data quality and authenticity to protect against data deterioration or degradation.

5.1.2. The Contractor shall also comply with the City's annual risk assessment requirements and associated security evaluation procedures.

5.2. **Audit Reports and Remediation**: The Contractor shall provide the City with all security audit reports, certifications, scan results, and executive summary of test documentation within seven (7) business days, upon request. The Contractor shall remediate identified vulnerabilities as follows: (i) critical vulnerabilities within thirty (30) days; (ii) high vulnerabilities within thirty (30) days; and (iii) medium and low vulnerabilities according to industry-standard timelines. The Contractor shall provide written evidence of completed remediation to the City upon request.

5.3. **Additional Security Assessments**: The City may request additional security audits, assessments, or testing beyond the baseline requirements if warranted by: (i) changes in the threat environment; (ii) Security Breaches or suspected security incidents; (iii) significant changes to the Work or systems; or (iv) results of baseline audits indicating material security deficiencies. For additional assessments required under subsections (i), (ii), or (iv), the Contractor shall bear the cost. For additional assessments required under subsection (iii) that result from City-requested changes to the scope of Work, the Parties shall negotiate cost responsibility in good faith. The Contractor shall provide results of all additional assessments to the City within seven (7) business days of receipt.

5.4. **Policy Disclosure**: Upon the City's request, the Contractor shall provide summary copies of its information security, data privacy, record retention, incident response, and business continuity policies and procedures applicable to the Work performed under this Agreement. The Contractor shall notify the City in writing of any material changes to such policies that could affect the Contractor's ability to meet its obligations under this Agreement.

6. DISASTER RECOVERY, BUSINESS CONTINUITY, AND TRANSITION

6.1. **Business Continuity and Disaster Recovery Program**: The Contractor shall maintain a business continuity and disaster recovery program designed to enable the Contractor to resume and continue performing its obligations under this Agreement following any significant business disruption. The program shall include appropriate backup systems, failover capabilities, and recovery procedures to minimize service interruptions. The Contractor shall provide the City with a copy of its disaster recovery plan summary upon request.

6.2. **Business Continuity Testing and Remediation**: The Contractor shall test its business continuity and disaster recovery capabilities at least annually to verify the program's effectiveness in resuming and continuing operations under this Agreement. The Contractor shall provide the City with test summaries or documentation upon request.

6.3. **Transition Assistance**: The Contractor acknowledges that the Work is vital to the City and must continue without interruption upon expiration or termination of this Agreement. Contractor will provide City with the same post-termination data retrieval assistance that Contractor generally makes available to all customers. Requests for Contractor to provide additional assistance in downloading or transferring City Data, including requests for Contractor's data egress service, will result in additional fees and Contractor will not warrant or guarantee data integrity or readability in the external system.

6.4. **Survival of Obligations**: The obligations set forth in this Section 6 shall survive the expiration or termination of this Agreement to the extent necessary to effectuate their purposes, including the Contractor's obligations to provide transition assistance and the City's rights to access escrowed materials under the conditions specified herein.

7. DELIVERY AND ACCEPTANCE

7.1. **Acceptance Process**: Deliverables shall be deemed accepted ("Acceptance") ten (10) days after delivery, if the City has not provided written notice of rejection or a Review Extension Notice (defined below). The City may extend the review period by providing written notice to the Contractor prior to the expiration of the initial ten (10) day period stating that its review is in progress (a "Review Extension Notice"). A Review Extension Notice shall extend the review period by an additional thirty (30) days. The City may reject a Deliverable if it materially deviates from the specifications and requirements in this Agreement. Rejection notices shall describe the nature of the deviation. Deemed acceptance under this Section applies only to Deliverables that materially conform to their applicable specifications at the time of delivery; a Deliverable that does not materially conform shall not be deemed accepted by the passage of time. Acceptance, whether express or deemed, shall not preclude the City from asserting claims based on: (a) latent defects that could not reasonably have been detected during the review period; (b) the Contractor's failure to conduct proper quality assurance prior to delivery; or (c) the Contractor's gross negligence or willful misconduct. Acceptance does not waive any warranties or other obligations under this Agreement, and payment of an invoice prior to Acceptance does not constitute acceptance or waiver of any rights.

7.2. **Rejection and Remediation**: Following rejection, the Contractor shall correct the deviation at its sole expense and redeliver the Deliverable within fifteen (15) days. The acceptance procedures above shall apply to redelivered Deliverables. If the City determines that a Deliverable does not perform as warranted after Acceptance, the City may revoke acceptance and require remediation in accordance with the warranty provisions of this Agreement..

7.3. **Quality Assurance**: The Contractor shall provide and maintain a quality assurance program acceptable to the City for all Deliverables under this Agreement. The Contractor shall deliver only Deliverables that have been inspected and verified to conform to the applicable specifications. Delivery of any Deliverable constitutes the Contractor's certification of conformance with specifications. The Contractor shall make quality assurance records available to the City upon request.

8. WARRANTIES AND REPRESENTATIONS

8.1. **Third-Party Warranties and Indemnities**: The Contractor shall assign to the City all third-party warranties and indemnities related to the Work, to the extent assignable. For non-assignable warranties, the Contractor shall enforce them on the City's behalf at the City's request. The Contractor shall provide the City with copies of all applicable third-party warranty terms upon request.

8.2. **Disabling Code Warranty**: The Contractor warrants that the Work does not and will not contain any malicious code, including without limitation viruses, worms, trojans, ransomware, backdoors, time bombs, logic bombs, or other code designed to damage, disrupt, disable, harm, or impede operation of any systems or data ("Disabling Code"). If Disabling Code is identified in the Work, the Contractor shall, at no cost to the City: (i) immediately contain and remove the Disabling Code; (ii) restore or reconstruct any City Data or systems affected by the Disabling Code; and (iii) provide the City with a corrected version of the Work and re-implement as necessary.

9. LICENSE AND USE AUDIT RIGHTS

9.1. **Applicability**: This Section applies to the extent the Contractor has granted the City any license or other limited permission to use the Contractor's intellectual property under this Agreement.

9.2. **Audit Request**: The Contractor may, no more than once per calendar year, request in writing that the City audit and certify its compliance with applicable license or use restrictions under this Agreement (an "Audit Request"). The Audit Request shall specify the period to be audited, which shall not overlap with any previously audited period. The City shall complete the audit and provide its certification ("Audit Certification") within ninety (90) days of receipt of the Audit Request.

9.3. **Overuse and Remediation**: If the Audit Certification reveals that the City's use exceeded the applicable license or use restrictions ("Overuse"), the Contractor shall provide written notice identifying the specific Overuse and any additional licenses, maintenance, or services required to bring the City into compliance. The City shall have sixty (60) days from receipt of such notice to cure the Overuse by either: (i) reducing its use to conform with the applicable restrictions; or (ii) purchasing additional licenses or services at the rates specified in this Agreement. The Contractor shall not impose retroactive fees, penalties, or assessments for any period preceding the Audit Request.

9.4. **Audit Protections**: The following protections apply to any audit conducted under this Section: (i) Any dispute regarding the results of an Audit Certification shall be resolved through the dispute resolution procedures in the Framework Agreement; (ii)

The Contractor shall treat all Audit Certifications and related communications as Confidential Information of the City; (iii) The Contractor shall not suspend, terminate, or degrade the City's access to the Work or Services based on an audit finding until the cure period in this Section has expired without cure; and (iv) The City may satisfy its audit obligations through electronic usage reports, system-generated license utilization data, or other remote verification methods, provided such methods reasonably demonstrate the City's compliance with the applicable restrictions.

REMAINDER OF PAGE INTENTIONALLY LEFT BLANK

EXHIBIT D, DEPARTMENT OF PUBLIC SAFETY INFORMATION TECHNOLOGY PROVISIONS

This Exhibit applies to all technology systems, software, hardware, and services procured by or on behalf of the City and County of Denver Department of Public Safety ("DPS") under this Agreement, including but not limited to law enforcement technology systems, public safety communications equipment, evidence management systems, analytics platforms, and any other information technology that processes, stores, or transmits Safety Data (as defined below).

This Exhibit regarding the DPS' Information Technology Provisions (this "Exhibit") is a material part of the Agreement between the Parties to which this Exhibit is attached. In addition to the requirements of the main body of this Agreement and **Exhibit C** (Information Technology Provisions), the Contractor shall comply with the specific requirements set forth in this Exhibit when providing technology systems or services to DPS. All provisions of this Exhibit that refer to the Contractor shall apply equally to any Subcontractor performing work in connection with this Agreement. Unless the context clearly requires a distinction between the Agreement and this Exhibit, all references to "Agreement" shall include this Exhibit.

1. **RELATIONSHIP TO OTHER PROVISIONS**: The requirements in this Exhibit are in addition to, and do not supersede or replace, the data protection and security requirements set forth in this Agreement and its **Exhibit C**. Where any provision of this Exhibit addresses the same subject matter as a provision in the main body of this Agreement or **Exhibit C**, the more protective provision for the City shall govern. In the event of any conflict between this Exhibit and other provisions of this Agreement with respect to DPS technology procurements, this Exhibit shall control.
2. **DEFINITIONS**: For purposes of this Exhibit, "Safety Data" means all City Data (as defined in Section 1.1 of this Agreement) that: (i) is generated by, processed through, stored in, or transmitted by any technology system provided under this Agreement for use by DPS; (ii) relates to public safety operations, law enforcement activities, emergency response, or criminal justice functions; or (iii) is accessed, used, or maintained by DPS personnel in performance of their official duties. Safety Data includes, without limitation, data captured by license plate readers, body-worn cameras, surveillance systems, evidence management systems, dispatch systems, analytics platforms, and any other public safety technology. For the avoidance of doubt, Safety Data is a subset of City Data as defined in this Agreement, and all protections applicable to City Data shall apply to Safety Data. The provisions of this Exhibit provide additional protections specific to Safety Data.
3. **CHANGE MANAGEMENT AND SYSTEM MODIFICATION CONTROLS**
   - 3.1. **Right to Opt-Out of System Changes**: Notwithstanding any provision in **Exhibit C** regarding software updates and upgrades, the City reserves the right to opt-out of or delay implementation of any new feature, functionality, update, upgrade, or system modification that would substantially alter: (i) the core functionality of the technology

system as described in the Specifications; (ii) the data collection, processing, storage, transmission, or sharing capabilities of the system; (iii) the operational use or workflow of the system by DPS personnel; (iv) the security architecture or access controls of the system; or (v) the integration with other City systems or third-party platforms (collectively, "Material System Changes").

3.2. **Advance Notice and Approval Requirements**: The Contractor shall provide the City with written notice at least thirty (30) days prior to any planned Material System Change. Such notice shall include: (a) a detailed description of the proposed change and its technical specifications; (b) an assessment of how the change will affect system functionality, data handling, and operational workflows; (c) any changes to data collection, processing, sharing, or retention that would result from the modification; (d) security implications and any impact on existing access controls or audit capabilities; (e) training requirements for DPS personnel; and (f) the Contractor's recommended implementation timeline. The City shall have thirty (30) days from receipt of such notice to approve, reject, or request modifications to the proposed Material System Change. The Contractor shall not implement any Material System Change without the City's express written approval.

3.3. **Non-Material Updates**: Updates or modifications that do not constitute Material System Changes (such as minor bug fixes, security patches addressing known vulnerabilities, or performance optimizations that do not alter functionality or data handling) may be implemented by the Contractor following ten (10) business days' written notice to the City, unless the City objects within such period. Emergency security patches addressing actively exploited vulnerabilities may be implemented immediately upon notice to the City, provided the Contractor delivers a detailed post-implementation report describing the vulnerability addressed and the changes made.

3.4. **Beta Features and Pilot Programs**: The City shall not be enrolled in any beta testing program, pilot feature rollout, or experimental functionality without the City's express written consent. The Contractor shall clearly identify any feature or functionality offered to the City as "beta," "pilot," "experimental," or similar designation, and shall provide the City with information regarding: (i) the stability and testing status of such feature; (ii) any data collection or processing associated with the feature; (iii) the City's ability to disable or opt-out of the feature; and (iv) the anticipated timeline for general availability or feature retirement.

4. EMERGENCY DISCLOSURE AND EXIGENT CIRCUMSTANCES POLICY

4.1. **Policy Disclosure Requirement**: Upon request , the Contractor shall provide the City with the applicable external facing written copy of the Contractor's notices regarding data processing. . The Axon Cloud Services Notice (attached as a Schedule 1 to this Exhibit) will provide overview on the following topics:

4.1.1. Requests from federal, state, or local law enforcement agencies or other governmental entities accompanied by a subpoena, warrant, court order, or other legal process;

4.1.2. Requests from federal, state, or local law enforcement agencies or other governmental entities without a subpoena, warrant, court order, or other legal process;

4.1.3. Emergency or exigent circumstances in which the Contractor may release data without legal process and without prior notice to or consent from the affected client; and

4.1.4. Any other circumstances under which the Contractor's policy permits or requires disclosure of data maintained on behalf of its clients to third parties, including but not limited to disclosures pursuant to the Contractor's terms of service, privacy policy, or data sharing agreements.

4.2. **Exigent Circumstances Definition and Authorization**: If the Contractor's policy permits release of Safety Data in emergency or exigent circumstances without prior City approval, the Contractor shall provide the City with:

4.2.1. A comprehensive list of the specific circumstances that the Contractor has defined as qualifying as "emergency," "exigent," or similar urgent situations justifying release of data without legal process or customer approval;

4.2.2. The job titles, roles, or positions within the Contractor's organization authorized to make the determination that exigent circumstances exist and to approve emergency data release;

4.2.3. The internal approval process and chain of command required before any emergency release is authorized;

4.2.4. The timeframe within which the Contractor will notify the City following any emergency release of Safety Data (which shall be no later than forty-eight (48) hours after such release);

4.2.5. The documentation and audit trail that the Contractor maintains for all emergency data releases.

4.3. **City Notification and Objection Rights**: The Contractor shall comply with the notification and cooperation requirements set forth in this Agreement for all requests for disclosure of Safety Data. In addition, the Contractor shall:

4.3.1. Provide the City with immediate notice (within twenty-four (24) hours) upon receipt of any request for disclosure of Safety Data, regardless of whether the request is accompanied by legal process;

4.3.2. Provide the City with copies of any subpoena, warrant, court order, or other legal process, and any written request from law enforcement or governmental entities, within forty-eight (48) hours of receipt;

4.3.3. Cooperate reasonably with the City in evaluating or responding to requests for disclosure, including, where permitted by law, providing advance notice prior to any production;

4.3.4. Direct requesting parties to the City or originating agency as the appropriate entity to respond to requests for Safety Data and, to the extent Contractor is legally required

to respond, assert applicable objections and limit any disclosure to the minimum information required by law; and

4.3.5. In the event of an emergency release under the Contractor's exigent circumstances, provide the City notice within a 48 hours, unless legally prohibited, including a general description of the information disclosed and the basis for the disclosure.

4.4. **Policy Review and Updates**: Upon request, the Contractor shall provide the City with an updated copy of its disclosure notice policy annually, and provide the following information (i) the personnel authorized to approve emergency releases; (ii) the types of requests to which the Contractor will respond without legal process; or (iii) any data sharing agreements or arrangements that could result in disclosure of Safety Data.

4.5. **Restriction on Emergency Federal Disclosures**: The Contractor shall not make any emergency release of Safety Data to a federal law enforcement agency, intelligence agency, or any entity of the federal government under its exigent circumstances policy without first making a good-faith attempt to reach the City's designated emergency contact. If contact cannot be made within two (2) hours of identifying the claimed exigent circumstance, the Contractor shall document that failure before proceeding with any disclosure. For purposes of this Section, release to federal immigration enforcement agencies shall never qualify as an exigent circumstance under this Agreement.

5. MULTI-TENANT ARCHITECTURE AND FEDERAL ACCESS DISCLOSURE

5.1. **Infrastructure and Architecture Disclosure**: Within thirty (30) days of the Effective Date of this Agreement, and annually thereafter upon written request, the Contractor shall provide the City with a written disclosure describing:

5.1.1. Whether the system or infrastructure on which Safety Data is stored, processed, or transmitted is shared with other entities (i.e., multi-tenant architecture versus dedicated infrastructure);

5.1.2. If multi-tenant, the technical and logical controls in place to segregate Safety Data from data belonging to other entities, including but not limited to encryption, access controls, network segmentation, and database partitioning;

5.1.3. A list of all other governmental entities, law enforcement agencies, or public safety organizations whose data is stored, processed, or transmitted on the same infrastructure, systems, or platforms as Safety Data;

5.1.4. Contractor warrants that no federal law enforcement agency, intelligence agency, or other federal governmental entity has: (i) direct access to the infrastructure, systems, databases, or platforms on which Safety Data resides; (ii) the technical capability to access Safety Data, whether or not such capability has been exercised; (iii) any contractual right to access data on such infrastructure, systems, or platforms; or (iv) any backdoor, administrative access, or other means of accessing Safety Data without the City's active involvement in each instance of access; and

5.1.5. A description of any legal obligations, including but not limited to national security letters, FISA orders, or other classified or non-public legal requirements, that obligate the Contractor to provide federal agencies with access to data maintained on the Contractor's infrastructure or to the infrastructure itself, to the extent the Contractor is legally permitted to disclose such obligations.

5.2. **Federal Agency Access Protocols**: If any federal law enforcement agency, intelligence agency, or other federal governmental entity has or obtains access to the infrastructure on which Safety Data resides, the Contractor shall:

5.2.1. Notify the City in writing within ten (10) business days of any new federal agency being granted access to such infrastructure, systems, or platforms, to the extent legally permissible;

5.2.2. Maintain detailed audit logs of all instances of federal agency access to any systems or infrastructure that could potentially access Safety Data, including the identity of the accessing agency, date and time of access, nature and scope of access, and data accessed or retrieved;

5.2.3. Provide such audit logs to the City upon request, to the extent legally permissible;

5.2.4. Implement technical controls to prevent federal agencies with access to shared infrastructure from accessing Safety Data unless specifically authorized by the City or required by valid legal process served on the City; and

5.2.5. Immediately (within twenty-four (24) hours) notify the City if the Contractor receives any legal process, request, or directive from a federal agency to provide access to Safety Data or to disable, modify, or bypass any technical controls protecting Safety Data, to the extent legally permissible.

5.3. **Cloud Service Provider Disclosures**: If the Contractor utilizes any third-party cloud service provider (e.g., Amazon Web Services, Microsoft Azure, Google Cloud Platform) to host, store, process, or transmit Safety Data, the Contractor shall disclose:

5.3.1. The identity of all such cloud service providers and the specific services provided by each;

5.3.2. The geographic location(s) where Safety Data is stored and processed;

5.3.3. Whether such cloud service provider has disclosed publicly or is known to provide federal agencies with direct access to data on its infrastructure; and

5.3.4. Any contractual provisions in the Contractor's agreement with such cloud service provider that relate to federal agency access, law enforcement requests, or government data sharing.

6. PROTECTION OF LEGALLY PROTECTED HEALTH-CARE ACTIVITY DATA

6.1.Definitions: For purposes of this Section:

6.1.1. "Legally Protected Health-Care Activity" has the meaning set forth in Colo. Rev. Stat. § 12-30-121(1)(d), and includes seeking, providing, receiving, or referring for; assisting in seeking, providing, or receiving; or providing material support for or traveling to obtain gender-affirming health-care services or reproductive health care that is not unlawful in Colorado.

6.1.2. "Colorado Shield Laws" means Colorado Executive Order D 2022 032, Colo. Rev. Stat. §§ 24-116-101 et seq., Colo. Rev. Stat. § 13-1-140.1, and related provisions of Colorado law protecting individuals engaged in Legally Protected Health-Care Activities.

6.2. **Statutory Obligations**: The Contractor acknowledges that as a person acting on behalf of the City, the Contractor is subject to Colo. Rev. Stat. § 24-116-101 and shall not provide Safety Data or expend resources to further any out-of-state investigation or, to the extent constitutionally permissible, any federal investigation or proceeding that seeks to impose civil or criminal liability or professional sanctions upon any person or entity for engaging in a Legally Protected Health-Care Activity.

6.3. **Prohibited Actions**: Nothing in this Agreement requires Contractor to disclose Safety Data in violation of applicable law. Contractor shall respond to legal requests for Safety Data consistent with applicable law, valid legal process, and court orders, and may require such requests to be directed to the City or originating agency that owns or controls the data

6.4. **Exception for Subject Requests:** Notwithstanding the foregoing, the Contractor may provide information in response to a written request from the individual who is the subject of an investigation or proceeding, consistent with Colo. Rev. Stat. § 24-116-102(2).

6.5. **Inapplicability**: This Section does not apply to investigations or proceedings concerning conduct that was unlawful under Colorado civil or criminal law at the time the conduct occurred. For clarity, if the healthcare services sought, provided, or received were lawful in Colorado when they occurred, the protections of this Section apply regardless of: (i) whether such conduct is or becomes unlawful in the jurisdiction where the investigation originates; or (ii) subsequent changes to Colorado law.

6.6. **Notice Requirements**: The Contractor shall:

6.6.1. Immediately (within twenty-four (24) hours) notify the City Attorney's Office of any subpoena, warrant, court order, or other legal demand for Safety Data that relates to or could reasonably be used to investigate a Legally Protected Health-Care Activity;

6.6.2. Provide such notice before producing responsive information where legally permissible ; and

6.6.3. Provide reasonable cooperation with the City in evaluating or responding to such legal process.

6.6.4. If the Contractor is required by a court of competent jurisdiction or administrative body to disclose City Data, the Contractor shall first notify the City and, prior to any disclosure, cooperate with the City's reasonable requests in connection with the City's right to intervene, quash, or modify the legal order, demand, or request, and upon request, provide the City with a copy of its response. Upon notice, the City will promptly coordinate with the Contractor regarding the preservation and disposition of any City Data and records relevant to any current or anticipated litigation. If the

City receives a subpoena, legal order, or other legal demand seeking data maintained by the Contractor, the City will promptly provide a copy to the Contractor. Upon notice and if required by law, the Contractor shall promptly provide the City with copies of its data required for the City to meet its necessary disclosure obligations.

6.7. **Subcontractor Flow-Down**: The Contractor shall incorporate the requirements of this Section into all subcontracts and require subcontractors to comply with these provisions.

6.8. **Material Breach**: The Contractor's violation of this Section constitutes a material breach of this Agreement. The City may terminate this Agreement immediately upon written notice if the Contractor violates this Section. The Contractor shall be liable to the City for all damages resulting from such breach, including but not limited to:

6.8.1. Any civil penalties imposed on the City under Colo. Rev. Stat. § 24-74-107 or other applicable law;

6.8.2. Reasonable attorney fees and costs incurred by the City in connection with any resulting investigation or legal proceeding; and

6.8.3. Any damages or penalties assessed against the City or City employees arising from the Contractor's violation.

7. UNAUTHORIZED SHARING PROHIBITION

7.1. **Prohibition on Unauthorized Sharing**: The Contractor acknowledges that Safety Data is highly sensitive and that unauthorized disclosure could compromise public safety operations, civil liberties, and community trust. Except as expressly authorized in this Agreement or required by applicable law, the Contractor shall not disclose, provide access to, sell, license, transfer, or otherwise make available any Safety Data to any third party, including but not limited to federal law enforcement agencies, intelligence agencies, state or local law enforcement agencies outside of those authorized by the City, commercial partners, other customers, or data brokers. This prohibition includes but is not limited to participation in federal data sharing programs, fusion centers, information sharing agreements, or public-private partnerships that would result in unauthorized access to Safety Data, except as required by federal law, court order, subpoena, or warrant directed to the City or the Contractor.

7.2. **Permitted Disclosures**: The following disclosures shall not constitute Unauthorized Sharing under this Section:

7.2.1. **Disclosure Required by Legal Process**: Disclosure pursuant to a valid subpoena, warrant, or court order directed to the Contractor with respect to Safety Data, provided the Contractor complies with all notification and cooperation requirements set forth in this Agreement and Section 4.3 of this Exhibit;

7.2.2. **Emergency Disclosures**: Disclosure in response to an exigent or emergency circumstance as defined in the Contractor's exigent circumstances policy disclosed pursuant to Section 4 of this Exhibit, provided the Contractor complies with all notification requirements set forth therein; and

7.2.3. **City-Authorized Disclosures**: Disclosure expressly authorized in writing by the City on a case-by-case basis, which authorization shall specify the recipient, the scope of data to be disclosed, the purpose, and any limitations or conditions.

7.2.4. **Geographic and Standards Limitations on Authorized Disclosures**: Notwithstanding Section 7.2.3, City-authorized disclosures of Safety Data to law enforcement agencies shall be limited to agencies that: (i) are organized under the laws of the State of Colorado; and (ii) have executed a written data-sharing agreement with the City that incorporates, at minimum, the data use restrictions, retention limitations, and re-disclosure prohibitions set forth in this Exhibit. The Contractor shall not disclose Safety Data to any agency that has not satisfied both conditions, even if directed by the City, and shall promptly notify the City Attorney if it receives such direction.

7.3. **Clarification Regarding City-Directed Access**: Access to Safety Data by City personnel, by personnel of other governmental entities specifically authorized in writing by the City, or through City-initiated queries, searches, or lookups using the system's user interface in accordance with the terms of this Agreement, shall not constitute Unauthorized Sharing. However, any automated or systematic sharing of Safety Data with third parties triggered by City's use of the system, unless expressly disclosed to and approved by the City in writing, shall constitute Unauthorized Sharing.

7.4. **Network Isolation of Safety Data**: The Contractor shall not include Safety Data, or any derivative thereof, in any cross-customer database, network-wide search index, federated query system, or shared data pool that is accessible to any party other than the City and personnel specifically authorized by the City. This prohibition applies regardless of whether the data is associated with the City's account identifier and regardless of whether City users can initiate queries against such a network. The Contractor shall provide the City with written certification annually confirming that Safety Data has not been included in any such system.

7.5. **Relationship to Security Breach**: For the avoidance of doubt:

7.5.1. Security Breach (as defined in this Agreement) encompasses unauthorized access, use, or disclosure resulting from compromise of security controls, whether intentional, accidental, or through third-party action. The Contractor's indemnification obligations under this Agreement apply to all Security Breaches.

7.5.2. Unauthorized Sharing under this Section refers specifically to the Contractor's intentional, knowing, or reckless disclosure or provision of access to Safety Data in violation of the prohibitions set forth in this Section.

7.5.3. A single event may constitute both a Security Breach and an Unauthorized Sharing, in which case the indemnification obligations and termination rights set forth in this Agreement shall apply.

8. LAW ENFORCEMENT REQUEST POLICY AND DATA DESTRUCTION POLICY

8.1. **Law Enforcement Request Policy**: Within thirty (30) days of the Effective Date of this Agreement, the Contractor shall provide the City with a complete written

copy of the Contractor's policy for responding to law enforcement requests for data maintained on behalf of its clients, including how such policy specifically applies to Safety Data. This policy shall address, at a minimum:

8.1.1. The types of law enforcement requests the Contractor will honor (e.g., only those with warrants, or also those with subpoenas, court orders, or administrative subpoenas);

8.1.2. The verification procedures the Contractor employs to authenticate the validity of law enforcement requests;

8.1.3. The Contractor's process for notifying affected clients, including the City with respect to Safety Data (including timing and method of notice);

8.1.4. Any circumstances under which the Contractor will challenge, object to, or seek to narrow the scope of law enforcement requests;

8.1.5. The Contractor's policy regarding requests for expedited or emergency production;

8.1.6. Whether the Contractor publishes transparency reports regarding law enforcement requests and, if so, the level of detail provided; and

8.1.7. Any fees or costs the Contractor charges to law enforcement agencies for production of data.

8.2. **Data Destruction Policy**: Contract will comply with retention and deletion standards developed within the Axon Cloud Service Notice (attached as Schedule 1)Axon will delete data 90 days after contract termination.

8.3. **Data Retention Limitations**: Setting retention periods for Safety Data remains exclusively with the City, which may, through its appointed cloud admin, set the retention period in its cloud service tenancy. City may, at any time and in its sole discretion, permanently delete any and all Safety Data. The permanent deletion will be performed in accordance with Axon Cloud Service Notice (Schedule 1).

9. COLORADO LAW COMPLIANCE AND IMMIGRATION ENFORCEMENT

9.1. **Reaffirmation of Immigration Enforcement Prohibition**: The requirements set forth in this Agreement regarding immigration enforcement prohibition shall apply with full force to all Safety Data. The Contractor acknowledges that Safety Data may be particularly sensitive with respect to immigration enforcement concerns due to the nature of law enforcement operations and data collection by DPS. The Contractor reaffirms its commitment not to use, disclose, or provide access to Safety Data for purposes of investigating for, participating in, cooperating with, or assisting in federal immigration enforcement, except as required by federal or state law, to comply with a court-issued subpoena, warrant, or order, or in connection with criminal investigations authorized by judicial process.

9.2. **Contractor Personnel Obligations**: The Contractor shall ensure that all personnel with access to Safety Data:(i) understand applicable confidentiality obligations and the sensitive nature of Safety Data and (ii) route requests for Safety Data through Contractor's established legal process procedures . The Contractor shall monitor and

enforce compliance with these requirements and remains fully responsible for all actions taken by such personnel with respect to Safety Data.

10. ADDITIONAL SECURITY AND COMPLIANCE REQUIREMENTS

10.1. **Enhanced Vendor Risk Assessment Compliance**: In addition to the security requirements set forth in this Agreement and **Exhibit C**, the Contractor shall meet or exceed the system security and policy requirements set forth in the City's Technology Services Vendor Risk Assessment ("VRA") applicable to the specific technology system or service being provided. The Contractor shall participate in periodic VRA reviews as requested by the City, which may occur annually or more frequently based on the sensitivity of Safety Data and the criticality of the system to public safety operations. At a minimum, the Contractor shall maintain the following certifications and standards throughout the Term: (i) SOC 2 Type 2 certification applicable to the LPR system; (ii) encryption of Safety Data at rest using AES-256 or an equivalent NIST-approved algorithm of equal or greater strength; (iii) encryption of Safety Data in transit using TLS 1.2 or higher; and (iv) compliance with the FBI CJIS Security Policy for all Safety Data that constitutes or interfaces with Criminal Justice Information. The Contractor shall not downgrade from any of these standards without sixty (60) days' prior written notice and the City's express written consent.

10.2. **CJIS Compliance Reaffirmation**: To the extent Safety Data includes or interfaces with CJI as defined in the FBI CJIS Security Policy, the Contractor shall comply with all requirements set forth in this Agreement. The Contractor acknowledges that many DPS technology systems involve CJI and that CJIS compliance is a material requirement of this Agreement for such systems.

10.3. **Cooperation with Department of Safety Audits**: In addition to the audit rights reserved to the City under this Agreement and **Exhibit C**, the Contractor shall cooperate with audits, inspections, and assessments conducted by or on behalf of DPS to verify compliance with this Exhibit. Such audits may include review of the Contractor's incident response capabilities. The Contractor shall provide DPS personnel or designees with access to relevant documentation, and personnel necessary to complete such audits, subject to reasonable security protocols and advance notice requirements.

11. SURVIVAL AND ENFORCEMENT

11.1. **Survival**: The obligations set forth in this Exhibit shall survive the termination or expiration of this Agreement to the extent necessary to protect Safety Data, ensure proper destruction of such data, and address any breaches or violations that occurred during the term of this Agreement.

11.2. **Material Terms**: The Contractor acknowledges and agrees that the requirements set forth in this Exhibit are material terms of this Agreement. Any violation of this Exhibit, including but not limited to: (i) unauthorized disclosure of Safety Data to federal agencies; (ii) failure to notify the City of law enforcement requests; (iii) implementation of Material System Changes without City approval; (iv) providing false or incomplete information in required disclosures; (v) failure to comply with exigent circumstances

notification requirements; or (vi) sharing, disclosing, or providing access to Safety Data to any federal law enforcement or intelligence agency without prior express written City authorization and without a valid court-issued warrant directed to the City; shall constitute a material breach of this Agreement entitling the City to exercise any and all remedies available under this Agreement, including termination for breach in accordance with this Agreement. Violations of items (i), (ii), and (vi) of this Section shall constitute material breach for which no cure period shall apply; the City may terminate this Agreement immediately upon written notice without affording the Contractor any opportunity to cure.

11.3. **No Waiver of Other Protections**: Nothing in this Exhibit shall be construed to limit, waive, or reduce any protections afforded to City Data or Safety Data under the main body of this Agreement, **Exhibit C**, or any other provision of this Agreement. All such protections remain in full force and effect and are supplemented by the additional requirements set forth in this Exhibit.

REMAINDER OF PAGE INTENTIONALLY LEFT BLANK

Schedule 1 – Axon Privacy Policy

AXON CLOUD SERVICES PRIVACY NOTICE

This Axon Cloud Services Privacy Notice ("**Notice**") applies only to the information that Axon Enterprise, Inc. and its other legal entities ("**Axon**" "**we**", "**us**", "**our**") collect from Customers and their users (collectively, "**Customer**" "**you**" and "**your**") and provide to Axon in connection with Customer's use of Axon Cloud Services (as defined below). Axon's marketing sites and other public websites are governed by the Axon Global Privacy Notice.

Unless otherwise provided in this Notice, this Notice is subject to the terms of the Master Services Purchasing Agreement, or other similar agreement, if any, between Axon and Customer ("**Agreement**"). A concept or principle covered in this Notice shall apply and be incorporated into all other provisions of the Agreement in which the concept or principle is also applicable, notwithstanding the absence of any specific cross-reference thereto. All capitalized terms referenced, but not defined, in this Notice shall have the meanings assigned to them in the Agreement.

By using Axon Cloud Services, Customer acknowledges that Customer has read and understands this Notice. Axon may occasionally update this Notice. When Axon posts changes, Axon will revise the "last updated" date at the top of this page. Customer's continued use of Axon Cloud Services will signify Customer's acknowledgement, and to the extent allowed by law agreement to and acceptance of any such changes.

Definitions

· "**Axon Cloud Services**" means Axon's web services hosted on evidence.com including Axon Evidence and other related offerings, including, without limitation, interactions between Axon Cloud Services and Axon Products (as defined below).

· "**Axon Products**" means:
(1) Axon Cloud Services;
(2) devices sold by Axon (including, without limitation, conducted energy weapons, cameras, sensors, and docking systems) (collectively, "**Axon Devices**");
(3) other software offered by Axon (including, without limitation, Axon Investigate, Axon Capture, Axon Evidence SYNC, Axon Device Manager, Axon View, Axon Interview, Axon Commander, Axon Uploader XT, and Axon View XL) (collectively, "**Axon Client Applications**"); and
(4) ancillary hardware, equipment, software, services, cloud-based services, documentation, and software maintenance releases and updates. Axon Products do not include any third-party applications, hardware, warranties, or the 'my.evidence.com' services.

"**Customer Data**" means:
(1) "Customer Content", which means data uploaded into, ingested by, or created in Axon

Cloud Services within Customer's tenant, including, without limitation, media or multimedia uploaded into Axon Cloud Services by Customer ("Evidence"); and
(2) "Non-Content Data", which means:

(a) "Customer Entity and User Data", which means Personal Data and non-Personal Data regarding Customer's Axon Cloud Services tenant configuration;
(b) "Customer Entity and User Service Interaction Data" which means data regarding Customer's interactions with Axon Cloud Services and Axon Client Applications;
(c) "Service Operations and Security Data", which means data within service logs, metrics and events and vulnerability data, including, without limitation: (i) application, host, and infrastructure logs; (ii) Axon Device and Axon Client Application logs; (iii) service metrics and events logs; and (iv) web transaction logs;
(d) "Account Data", which means information provided to Axon during sign-up, purchase, or administration of Axon Cloud Services, including, without limitation, the name, address, phone number, and email address Customer provides, as well as aggregated usage information related to Customer's account and administrative data associated with the account; and
(e) "Support Data", which means the information Axon collects when Customer contacts or engages Axon for support, including, without limitation, information about hardware, software, and other details gathered related to the support incident, such as contact or authentication information, chat session personalization, information about the condition of the machine and the application when the fault occurred and during diagnostics, system and registry data about software installations and hardware configurations, and error-tracking files.

· **"Data Controller"** means the natural or legal person, public authority, or any other body which alone or jointly with others determines the purposes and means of the processing of Personal Data (as defined below).

· **"Data Processor"** means a natural or legal person, public authority or any other body which processes Personal Data on behalf of the Data Controller.

· **"Personal Data"** means information about or relating to an individual, whether recorded or not, whether or not true or factual, which can be used to uniquely identify the individual either on its own or by reference to an identifier such as an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

· **"Sensitive Personal Data"** means any information related to genetic, biometric and health data, as well as personal data revealing racial and ethnic origin, political opinions, religious or ideological convictions or trade union membership. Specific information types connected to an individual where misuse could negatively impact fundamental rights and

freedoms of the data subject. This includes financial data of an individual, racial, genetic, health or lifestyle data.

· "**Processing**" means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as

· collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

· **"Sub-processor"** means any third party engaged by the Data Processor to assist in data processing activities that the Data Processor is carrying out on behalf of the Data Controller.

Axon's Role

Data Processor

Axon is a Data Processor of Customer Content and Axon obtains no rights to Customer Content. The Customer is a Data Controller and controls and owns all right, title, and interest in and to Customer Content. Axon only processes Customer Content on behalf of the Customer in accordance with the Agreement and the Data Processing Agreement entered into between the parties.

Data Controller

Axon is a Data Controller for Non-Content Data. In regard to Customer Entity & User Data, Axon is a Data Controller and Customer is an independent Data Controller, not a joint Data Controller.

Axon processes Non-Content Data to provide Axon Cloud Services and to support the overall delivery and improvement of Axon Products including business, operational, and security purposes. Axon may analyze and report anonymized and aggregated Non-Content Data to communicate with external and internal stakeholders.

Data Collection Purposes and Processing Activities

Customer Content

Axon will only process Customer Content to provide Customer Axon Cloud Services including, without limitation, user authentication and authorization functionality, and to enable the functionalities according to the configuration selected by the Customer. Axon only processes Customer Content on behalf of the Customer in accordance with the Agreement and the Data Processing Agreement entered into between the parties. Axon will not use Customer Content for any advertising or other commercial purposes.

Axon periodically upgrades or changes Axon Cloud Services to provide customers with new

features and enhancements in alignment with the Axon Evidence Maintenance Schedule. Axon communicates such upgrades or changes to customers one week prior to release via mechanisms outlined in the Maintenance Schedule.

Non-Content Data

Axon processes Non-Content Data to provide Axon Cloud Services and to support the overall delivery of Axon Products including business, operational, and security purposes.

Non-Content Data includes the following:

Customer Entity and User Data

Axon uses Customer Entity and User Data to: (1) provide Axon Cloud Services, including, without limitation, user authentication and authorization functionality; (2) improve the quality of Axon Products or provide enhanced functionality and features; (3) contact Customer to provide information about its account, tenant, subscriptions, billing, and updates to Axon Cloud Services, including, without limitation, information about new features, security and other technical issues; and (4) market our products or services to Customer via email, by sending promotional communication including targeted advertisements, or presenting a Customer with relevant offers.

Customer cannot unsubscribe from non-promotional communications, such as maintenance schedules, or similar notifications, but may unsubscribe from promotional communications at any time such as by clicking on an unsubscribe button at the bottom of such communications.

Customer Entity and User Service Interaction Data

Customer Entity and User Service Interaction Data includes data regarding Customers' interactions with Axon Cloud Services and Axon Client Applications. Axon processes Customer Entity and User Service Interaction Data to improve the quality of Axon Products and provide enhanced functionality and features.

Service Operations and Security Data

Axon processes "Service Operations and Security Data" to provide service operations and monitoring for its own purposes of ensuring the security of its services and systems. The processing of "Service Operations and Security Data" is necessary for Axon to monitor the security of its services, detect vulnerabilities, and act promptly on security breaches. Therefore, the processing is necessary to meet Axon's legal obligations, to maintain security standards and to fulfil our contractual commitments to the Customer.

Account Data

Axon uses Account Data to provide Axon Cloud Services, manage Customer's accounts, to market, and communicate with Customer by carrying out the administrative management of

your registration and/or updating as a client, and the management and development of the contractual relationship with Customer and to contact Customer to provide information about its account, tenant, subscriptions, billing and updates to Axon Cloud Services, and to market our products or services to Customer via email, by sending promotional communications, including targeted advertisements, or by presenting Customer with relevant offers.

Support Data

Axon uses Support Data to resolve Customer's support incident, and to operate, improve, and personalize Axon Products, including, without limitation, information about hardware, software, and other details gathered related to the support incident, such as contact or authentication information, chat session personalization, information about the condition of the device and the application when the fault occurred and during diagnostics, system and registry data about software installations and hardware configurations, and error-tracking files. Service Operations and Security Data may be part of the Support Data when required for this purpose.

If Customer shares Customer Content to Axon in a support scenario, or access to or processing of Customer Content is necessary to provide support, the Customer Content will be processed as Support Data and will only be used for resolving support incidents.

Axon may provide support through phone, email, online chat or sessions. Phone conversations, online chat sessions, or online sessions with Axon support professionals may be recorded and/or monitored for efforts such as training, future support, and evidentiary purposes.

Legal Basis for Processing Personal Data

CUSTOMER CONTENT

Axon's legal basis for the collection and processing of Personal Data within Customer Content is to fulfill obligations to facilitate and process contractual transactions that take place when you interact with Axon Cloud Services.

NON-CONTENT DATA

Axon's legal basis for the collection and processing of Personal Data within Non-Content Data is the legitimate interest to provide and support the delivery of our Services; investigate and help prevent security threats, fraud, or other malicious activity; enforce & protect the rights and properties of Axon or its affiliates; protect the rights and personal safety of Axon employees and third parties on or using the Services or Axon Products; and for the purposes which may be required by applicable laws and regulations.

Server and Data Location

Customer Content

Axon offers Axon Cloud Services in numerous geographic regions. Before creating an account, Customer determines where Axon will store Customer Content by designating an economic area.

REGION CODE	ECONOMIC AREA	3RD PARTY INFRASTRUCTURE SUB-PROCESSORS	DATA CENTER LOCATION(S)
AU	Southeast Asia	Microsoft Azure	Canberra, ACT
LA	South America	Microsoft Azure	Sao Paulo, Brazil & Rio de Janeiro, Brazil or Sao Paulo, Brazil & *Texas, United States *new customers will not be added to the Texas, United States datacenter
CA	Canada	Microsoft Azure	Toronto, ON & Quebec City, QC
EU	European Union	Amazon Web Services	Ireland **new customers will not be added to this region
EUR	European Union	Microsoft Azure	Netherlands, Ireland
UK	United Kingdom	Microsoft Azure	London, England & Cardiff, Wales
US	United States	Microsoft Azure and Amazon Web Services	Texas, Virginia & Oregon, United States
US	United States (Federal Region)	Microsoft Azure	Texas & Virginia, United States
ENT	Global	Microsoft Azure and Amazon Web Services	Washington, Wyoming & Oregon, United States

Axon ensures that all Customer Content in Axon Evidence remains within the selected economic area, including, without limitation, all backup data, replication sites, and disaster recovery sites. Customer selected economic areas can be determined through review of Customer's Axon Cloud Services URL. Customer URLs conform to the *<youragency>.<regioncode>.evidence.com* scheme with the exception of US customers where the scheme may exclude the region code and is *<youragency>.evidence.com*. US Federal customers conform to the scheme *<youragency>.us.evidence.com*

Non-Content Data

Customer Entity and User Data

Customer Entity and User Data is located in Customer's selected economic area for Customer Content. Customer Entity and User Data may be copied or transferred to the United States.

Customer Entity and User Service Interaction Data

Customer Entity and User Service Interaction Data is located in Customer's selected economic area for Customer Content and the United States.

Service Operations and Security Data

Service Operations and Security Data is located in Customer's selected economic area for Customer Content and the United States.

Account Data and Support Data

Account and Support Data may be located in the United States and may be located in Customer's selected economic area for Customer Content.

Axon Cloud Services Sub-processors

Axon may rely on Sub-processors to provide or enhance Axon Products on its behalf. Axon only permits Sub-processors to use Customer Content to deliver to the Customer services that Axon offers. Axon prohibits Sub-processors from using Customer Content for any other purpose. Ownership of rights, titles, and interest in and to Customer Content remain with Customer.

Axon exercises commercially reasonable efforts in connection with contractual obligations to ensure its Sub-processors are compliant with all applicable data protection laws and regulations surrounding the Sub-processors access and scope of work in connection with Customer Content. Prior to onboarding Sub-processors, Axon audits the security and privacy practices of Sub-processors to ensure Sub-processors provide a level of security and privacy appropriate to the scope of their services.

Axon maintains an up-to-date list of the names and locations of the required Customer Content sub-processor(s) used to for standard Axon Cloud Services here. Please note, additional Sub-processors may be included depending on additional functionality requested during contracting and implementation. If additional information is needed, please contact Axon at privacy@axon.com.

Axon will give Customer notice of any new Sub-processor. If you are a current Axon Cloud Services customer with a data processing agreement in place with Axon, you may subscribe here to receive notifications of a new Sub-processor(s) before Axon authorizes any new Sub-processor to process Customer Content in connection with the provision of your service.

International Data Transfers

Personal Data within Non-Content Data may be subject to international data transfers outside the European Economic Area (EEA), United Kingdom, and Switzerland, which will be regulated in accordance with the mechanisms set out in the GDPR, UK-GDPR, and the Swiss FADP respectively, to safeguard the rights and freedoms of the data subject and ensure a level of protection equivalent to that required by European, United Kingdom, and Swiss regulations.

Axon and Fusus Inc. (‘Axon’) comply with the EU-U.S. Data Privacy Framework (EU-U.S. DPF), the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF) as set forth by the U.S. Department of Commerce. Axon has certified to the U.S. Department of Commerce that it adheres to the EU-U.S. Data Privacy Framework Principles (EU-U.S. DPF Principles) with regard to the processing of personal data received from the European Union in reliance on the EU-U.S. DPF and from the United Kingdom (and

Gibraltar) in reliance on the UK Extension to the EU-U.S. DPF. Axon has certified to the U.S. Department of Commerce that it adheres to the Swiss-U.S. Data Privacy Framework Principles (Swiss-U.S. DPF Principles) with regard to the processing of personal data received from Switzerland in reliance on the Swiss-U.S. DPF.

If there is any conflict between the terms in this Notice and the EU-U.S. DPF Principles and/or the Swiss-U.S. DPF Principles, the Principles shall govern. To learn more about the Data Privacy Framework (DPF) program, and to view our certification, please visit https://www.dataprivacyframework.gov/.

In compliance with the EU-U.S. DPF, the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. DPF, Axon commits to resolve DPF Principles-related complaints about our collection and use of your personal information. EU, UK, and Swiss individuals with inquiries or complaints regarding our handling of personal data received in reliance on the EU-U.S. DPF, the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. DPF should first contact Axon at privacy@axon.com.

In compliance with the EU-U.S. DPF, the UK Extension to the EU-U.S. DPF and the Swiss-U.S. DPF, Axon commits to cooperate and comply respectively with the advice of the panel established by the EU data protection authorities (DPAs), the UK Information Commissioner's Office (ICO) and the Gibraltar Regulatory Authority (GRA), and the Swiss Federal Data Protection and Information Commissioner (FDPIC) with regard to unresolved complaints concerning our handling of personal data received in reliance on the EU-U.S. DPF, the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. DPF.

If your DPF complaint cannot be resolved through the above channels, under certain conditions, you may invoke binding arbitration for some residual claims not resolved by other redress mechanisms.

If you are an EU, Swiss or UK Individual, where we transfer your personal data to third party service providers (see above) who perform services for us or on our behalf, we are responsible for the processing of that data by them and shall remain liable if they process your personal data in a manner inconsistent with the DPF Principles referred to below, unless we prove that we are not responsible for the event giving rise to the damage.

Axon is subject to the investigatory and enforcement powers of the United States Federal Trade Commission regarding compliance with the EU-U.S. Data Privacy Framework (EU-U.S. DPF) and the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF).

To the extent the above mechanisms cannot be used to adequately safeguard transfers outside the EEA, United Kingdom, or Switzerland, Axon will put in place alternate safeguards, as appropriate (such as Standard Contractual Clauses (SCCs) and Transfer Impact Assessments (TIA).

Information Sharing

Axon may share data with its subsidiaries, legal entities, third party service providers and other partners to help us operate, including for providers to facilitate: (1) user account management, authentication, analytics, and communication, (2) product features, e.g. product development, and error analytics, (3) customer service and support, and (4) security monitoring and investigation.

Required Disclosures

Axon will not disclose Customer Content or Non-Content Data to Government Authorities except as required by any law or regulation. If permitted, Axon will notify Customer if any disclosure request is received for Customer Content so Customer may challenge or object.

Data Security Measures

Axon is committed to helping protect the security of Customer Data. Axon has established and implemented policies, programs, and procedures that are commercially reasonable and in compliance with applicable industry practices, including administrative, technical, and physical safeguards to protect the confidentiality, integrity and security of Customer Content and Non-Content Data against unauthorized access, use, modification, disclosure, or other misuse.

Axon will take appropriate steps to ensure compliance with the data security measures by its employees, contractors, and Sub-processors, to the extent applicable to the respective scope of performance.

Additional information regarding Axon's Data Security program can be found by visiting https://trust.axon.com

Confidentiality

Customer Content and Non-Content Data is encrypted in transit over public networks. Customer Content is encrypted at rest in all Axon Cloud Service regions.

Axon protects all Customer Content and Non-Content Data with strong logical access control mechanisms to ensure only users with appropriate business needs have access to data. Third-party specialized security firms periodically validate access control mechanisms. Access control lists are reviewed periodically by Axon.

Integrity

As Evidence is ingested into Axon Cloud Services, a Secure Hash Algorithm ("SHA") checksum is generated on the upload device and again upon ingestion into Axon Cloud Services. If the SHA checksum does not match, the upload will be reinitiated. Once upload of Evidence is successful, the SHA checksum is retained by Axon Cloud Services and is made

viewable by users with access to the Evidence audit trail for the specific piece of Evidence. Tamper-proof audit trails are created automatically by Axon Cloud Services upon ingestion of any Evidence.

Availability

Axon takes a comprehensive approach to ensure the availability of Axon Cloud Services. Axon replicates Customer Content over multiple systems to help to protect against accidental destruction or loss. Axon Cloud Services systems are designed to minimize single points of failure. Axon has designed and regularly plans and tests its business continuity planning and disaster recovery programs.

Isolation

Axon logically isolates Customer Content. Customer Content for an authenticated customer will not be displayed to another customer (unless Customers explicitly create a sharing relationship between their tenants or shared data between themselves). Centralized authentication systems are used across an Axon Cloud Service region to increase uniform data security.

Additional role-based access control is leveraged within Customer's Axon Cloud Service tenant to define what users can interact with or access Customer Content. Customer solely manages the role-based access control mechanisms within its Axon Cloud Services tenant.

Within the Axon Cloud Services supporting infrastructure, access is granted based on the principle of least privilege. All access must be approved by system owners and undergo at least quarterly user access reviews. Any shared computing or networking resource will undergo extensive hardening and is validated periodically to ensure appropriate isolation of Customer Content.

Non-Content Data is logically isolated within information systems such that only appropriate Axon personnel have access.

Personnel

Axon personnel are required to conduct themselves in a manner consistent with applicable law, the company's guidelines regarding confidentiality, business ethics, acceptable usage, and professional standards. Axon personnel must complete security training upon hire in addition to annual and role-specific security training.

Axon personnel undergo an extensive background check process to the extent legally permissible and in accordance with applicable local labor laws and statutory regulations. Axon personnel supporting Axon Cloud Services are subject to additional role-specific security

clearances or adjudication processes, including Criminal Justice Information Services background screening and national security clearances and vetting.

Data Breach

Notification

If Axon becomes aware of unlawful or unauthorized access to, disclosure, alteration, or destruction of Non-Content or Customer Data, we will notify affected Customers and relevant authorities as necessary.

Data Portability, Migration, and Transfer Back Assistance

Data Portability

Evidence uploaded to Axon Cloud Services is retained in original format. Evidence may be retrieved and downloaded by Customer from Axon Cloud Services to move data to an alternative information system. Evidence audit trails and system reports may also be downloaded in various industry-standard, non-proprietary formats.

Data Migration

In the event Customer's Axon Cloud Services is terminated, Axon will not delete any Customer Content during the 90 days following termination. During this 90-day period, Customer may retrieve Customer Content only if Customer has paid all amounts due (there will be no application functionality of the Axon Cloud Services during this 90-day period other than the ability for Customer to retrieve Customer Content). Customer will not incur any additional fees if Customer downloads Customer Content from Axon Cloud Services during this 90-day period. Axon has no obligation to maintain or provide any Customer Content after the 90-day period and thereafter, unless legally prohibited, will delete Customer Content upon termination as part of normal retention and data management instructions from customers. Upon written request, Axon will provide written proof that all Customer Content has been successfully deleted and removed from Axon Cloud Services.

Post-Termination Assistance

Axon will provide Customer with the same post-termination data retrieval assistance that is generally made available to all customers. Requests for additional assistance to Customer in downloading or transferring Customer Content will result in additional fees and Axon cannot warrant or guarantee data integrity or readability in the external systems.

Children's online privacy protection

Axon takes seriously its obligations under the Children's Online Privacy Protection Act. We do not knowingly collect Non-Content Data regarding children under 18.

Data Subject Rights

Non-Content Data

You have the rights described below with respect to your Personal Data. You may have the rights described below:

· Access and obtain a copy of your Personal Data on request;

· Require Axon to change incorrect or incomplete Personal Data;

· Require Axon to delete or stop processing your Personal Data, for example where the Personal Data is no longer necessary for the purposes of processing;

· Object to the processing of your Personal Data where Axon is relying on its legitimate interests as the legal ground for processing; and

· Withdraw your consent in circumstances where consent is the legal basis for processing.

If you would like to exercise any of these rights or have any questions, please contact us at privacy@axon.com. To submit a deletion request, please complete this form.

If you believe that Axon has not complied with your data protection rights, you may have the right to lodge a complaint with a supervisory authority, in particular in the jurisdiction where you work, normally live or where any alleged infringement of data protection laws occurred.

In the EEA: the data protection authority of their place of residence;

In the United Kingdom: the UK Information Commissioner's Office ("ICO");

In Switzerland: the Federal Data Protection and Information Commissioner ("FDPIC").

In the United States, please contact your applicable State Attorney General.

In other locations around the world, their local data protection authority.

If personal data covered by this Privacy Notice is to be used for a new purpose that is materially different from that for which the personal data was originally collected or subsequently authorized, or is to be disclosed to a non-agent third party in a manner not specified in this policy, Axon will provide you with an opportunity to choose whether to have your personal data so used or disclosed. Requests to opt out of such uses or disclosures of Personal Data should be sent to us as specified in the "How to Contact Us" section below.

Certain personal data, such as information about medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, is considered "Sensitive Information." Axon will not use Sensitive Personal for a purpose other than the purpose for

which it was originally collected or subsequently authorized by the individual unless Axon has received your affirmative and explicit consent (opt-in).

Customer Content

Customers may process Personal Data regarding an individual when leveraging Axon Cloud Services. In such cases, we are processing such personal data purely on behalf of our Customers and any individuals who seek to exercise their rights should first direct their query to our Customer, the Data Controller.

Axon will work with Customers to provide access to Personal Data that Axon or Sub-processors hold. Axon will also take reasonable steps to enable Customers to correct, amend, or delete Personal Data that is demonstrated to be inaccurate.

Data Retention

Customer Content

Customer defines Evidence retention periods pursuant to Customer's internal retention policies and procedures. Customer can establish its retention policies within Axon Cloud Services. Therefore, Customer controls the retention and deletion of its Evidence within Axon Cloud Services.

Non-Content Data

Axon maintains internal disaster recovery and data retention policies in accordance with applicable laws and regulations. The disaster recovery plan relates to Axon's data and extends to Axon Cloud Services and Customer Content stored within.

Axon's data retention policies relate to Axon's Non-Content Data. Axon's data retention policies instruct for the secure disposal of Non-Content Data when such data is no longer necessary for the delivery and support of Axon products and services and in accordance with applicable regulations. We will retain Non-Content Data for as long as needed to provide services, comply with our legal obligations, resolve disputes, and enforce our agreements.

Your California Privacy Rights

Pursuant to the California Consumer Privacy Act ("CCPA"), as amended by the California Privacy Rights Act ("CPRA"), we provide this California Consumer Privacy Act Addendum (the "CCPA Addendum") to California residents ("consumers" or "you" or "your"). This CCPA Addendum supplements the information contained in our Axon Cloud Services Privacy Notice. Any capitalized term used but not defined in this Notice has the meaning given in our Axon Cloud Services Privacy Notice.

This CCPA Addendum does not apply to information we collect about individuals in their capacity as present or former job applicants or employees of Axon or the use of the Axon

website. Nor does this amendment cover processing of Customer Content within Axon Cloud Services.

Categories of Personal Information Collected

Categories of Personal Information	Examples
Identifiers and Contact Information	Name, postal address, telephone number, unique personal identifier, online identifier, Internet Protocol address, username, email address or other similar identifiers
Commercial Information	Records and history of products or services purchased or considered
Internet or other electronic network activity information	Interaction with our websites, applications, or advertisements
Geolocation data	Approximate physical location (derived from an Internet Protocol address)
Professional or employment-related information	Job title, employer name. Inferences drawn from the any of the above
Account authentication credentials	Username, encrypted and hashed password

Sources of Personal Information

We obtain the categories of Personal Information listed above directly from you as well as from the following categories of sources: our corporate affiliates, third-party business partners, and other third-party sources.

Use of Personal Information

We use Personal Information for a variety of business and commercial purposes, as described this Axon Cloud Services Privacy Notice.

Your Consumer Rights under the CCPA

California law grants state residents certain rights, including the rights to know and access specific types of Personal Data, to learn how we process Personal Data, to request deletion of Personal Data, to request correction of Personal Data, to opt-out of sharing your Personal Data for third party advertising purposes, and not to be denied goods or services for exercising these rights.

If you would like to exercise any of these rights please contact us at privacy@axon.com.

Right to Opt-Out of Selling or Sharing

In the preceding 12 months, Axon has not sold or shared (as those terms are defined in the CCPA) any Personal Data.

Authorized Agents

To make a request as an authorized agent on behalf of a California resident, you may use the submission methods noted above. Please provide us with a copy of the consumer's written authorization designating you as their agent.

Nondiscrimination

We will not unlawfully discriminate against you for exercising your rights under the CCPA.

Additional Information about specific Axon Cloud Services

The following information pertains to specific privacy and data processing activities associated with certain Axon Cloud Services. If you are a user of any of the below products, please read the applicable language carefully.

Community Request

Community Request services may facilitate the transmission of information and content voluntarily submitted including certain metadata associated therewith, (collectively, "**Submissions**") by an individual completing questionnaires, while using Community Request **("Survey Participant"),** to our Customer that uses the Community Request service. Our Customer which requests Submissions through Community Request receives those Submissions - once transmitted, the Submissions remain in the possession of the requesting Customer and Axon does not own or control any copies. The Customer is thus the Data Controller of Submissions data. The Customer to which a Survey Participants transmits the Submission will own and control such Submission, and the privacy practices of Axon's Customer will apply.

Additionally, Community Request automatically collects certain details about a Survey Participant usage of Community Request and their device. Axon may automatically collect certain details of your access to and use of Community Request, including traffic data, location data, logs, and other communication data and the resources that you access and use on or through Community Request. We may collect information about your mobile device and internet connection, including the operating system, IP address, browser type, and mobile network information.

My90

My90 services may facilitate the transmission of information and content voluntarily submitted including certain metadata associated therewith, (collectively, "**Submissions**") by an individual completing questionnaires, while using My90 **("Survey Participant"),** to our Customer that

uses the My90 service. Survey Participants should not submit Personal Data as part of a Submission. If Personal Data is submitted, Axon will remove or de-identify the Submission.

Axon will analyze and aggregate Submissions to evaluate Customer interactions with respondents or to obtain insight. For example, this is done to understand the effectiveness of existing emergency response processes or to understand sentiment towards My90 Customers. This information can help Axon, and its Customers obtain insights and comparison on community trends and accordingly implement or recommend implementation of measures to improve policing.

Axon may also share aggregated Submissions publicly or privately through various mediums. We share this information to provide insights and comparisons on general policing and community trends. Prior to sharing this information, Axon will ensure that the Submission has been aggregated and de-identified so it can no longer be linked directly to a respondent.

Outside of the usage of Submissions, My90 automatically collects certain details about a Survey Participant usage of My90 and their device. Axon may automatically collect certain details of your access to and use of My90, including traffic data, location data, logs, and other communication data and the resources that you access and use on or through My90. We may collect information about your mobile device and internet connection, including the operating system, IP address, browser type, and mobile network information.

Axon Fusus

We process Customer Content on behalf of and as a Data Processor, and to the extent necessary to provide Services to our Customers. To provide our Customers with our Services, we may process and store Customer Content that is captured and recorded when our Customers and their users operate our Products and other Services, such as video or audio recordings, live video or audio streams, images, comments, and data our products collect from their surrounding environment to perform their functions (such as motion, events, temperature and ambient light). The Customer is thus the Data Controller of Customer Content collected by Fusus and the privacy practices of Axon’s Customer will apply.

Axon Fusus Terms of Use prohibits the use of cameras set by our Customers with our Platform or other Services in locations where a person has a reasonable expectation of privacy. We require our Customers to conduct any video monitoring through our Services in compliance with applicable laws, regulations and policies, including non-discrimination, sexual harassment, among others. Therefore, monitoring in the bathrooms, locker rooms, or other areas where individuals have a reasonable expectation of privacy is prohibited;

Axon Fusus Terms of Use also specifies that the camera positions and views are limited to open, common and public areas, unless otherwise permitted by a court order authorized by a court of competent jurisdiction relating to an investigation by a law enforcement agency.

Additionally, Axon Fusus may automatically collect certain details about users of Axon Fusus Products or Services. Axon may automatically collect certain details of your access to and use of Axon Fusus Products or Services, including traffic data, location data, logs, and other communication data and the resources that you access and use on or through Axon Fusus Products or Services.

How to Contact Us

If you have any questions or concerns regarding Axon's privacy practices or the content of this Notice, please contact privacy@axon.com.

EXHIBIT E, FEDERAL BUREAU OF INVESTIGATION
CRIMINAL JUSTICE INFORMATION SERVICES
SECURITY ADDENDUM

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

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

This Security Addendum identifies the duties and responsibilities with respect to the installation and maintenance of adequate internal controls within the contractual relationship so that the security and integrity of the FBI's information resources are not compromised. The security program shall include consideration of personnel security, site security, system security, and data security, and technical security.

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

1.00 Definitions

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

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

2.00 Responsibilities of the Contracting Government Agency.

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

3.00 Responsibilities of the Contractor.

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

4.00 Security Violations.

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

4.02 Security violations can justify termination of the appended agreement.

4.03 Upon notification, the FBI reserves the right to:

a. Investigate or decline to investigate any report of unauthorized use;

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

5.00 Audit

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

6.00 Scope and Authority

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

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

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

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

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

Information Security Officer

Criminal Justice Information Services Division, FBI

1000 Custer Hollow Road

Clarksburg, West Virginia 26306

FEDERAL BUREAU OF INVESTIGATION
CRIMINAL JUSTICE INFORMATION SERVICES
SECURITY ADDENDUM

CERTIFICATION

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

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

Charles Fehrman Signed by: 8774DEA8AD2943E... 2/19/2025 | 10:23 AM MST

Printed Name/Signature of Contractor Employee Date

Benjamin Hagen 2/19/2025 | 10:23 AM MST

Printed Name/Signature of Contractor Representative Date

Axon Enterprise, Inc. / CISO

Organization and Title of Contractor Representative

This Exhibit F is attached to and made a part of Framework Agreement No. 202683606 between the City and County of Denver and Axon Enterprise, Inc. (the "Agreement"). This Exhibit is incorporated into the Agreement as of the Effective Date and is subject to all terms and conditions of the Agreement. In the event of any conflict or inconsistency between this Exhibit and the Agreement, the Agreement controls in accordance with the Order of Precedence set forth in § 31 thereof. This Exhibit applies solely to the City's purchase and use of the Axon devices and services identified in the applicable Quote. All capitalized terms used but not defined in this Exhibit have the meanings given to them in the Agreement. This Exhibit does not create an independent contractual relationship between the Parties and may not be construed as a standalone agreement. No term, condition, or provision of this Exhibit modifies, waives, or supersedes any provision of the Agreement unless expressly agreed to by both Parties in a written amendment executed by authorized representatives.

1. **Definitions.**

   1.1. "**Axon Cloud Services**" means Axon's web services, but excludes third-party applications, hardware warranties, and my.evidence.com.

   1.2. "**Axon Device**" means all hardware provided by Axon under this Agreement. Axon-manufactured Devices are a subset of Axon Devices.

   1.3. "**Quote**" means an offer to sell and is only valid for devices and services on the offer at the specified prices. Any inconsistent or supplemental terms within Customer's purchase order in response to a Quote will be void. Orders are subject to prior credit approval. Changes in the deployment estimated ship date may change charges in the Quote. Shipping dates are estimates only. Axon is not responsible for typographical errors in any Quote by Axon, and Axon reserves the right to cancel any orders resulting from such errors.

   1.4. "**Services**" means all services provided by Axon under this Agreement, including software, Axon Cloud Services, and professional services.

2. **Term.** This Agreement begins on the Effective Date and continues until all subscriptions hereunder have expired or have been terminated ("**Term**").

   2.1. All subscription plans begin on the date stated in the Quote. Each subscription term ends upon completion of the subscription stated in the Quote ("**Subscription Term**").

3. **Taxes.** Customer is responsible for sales and other taxes associated with the order unless Customer provides Axon a valid tax exemption certificate.

4. **Shipping.** Axon may make partial shipments and ship Axon Devices from multiple locations. All shipments are EXW (Incoterms 2020) via common carrier. Title and risk of loss pass to Customer upon Axon's delivery to the common carrier. Customer is responsible for any shipping charges in the Quote.

5. **Returns.** All sales are final. Axon does not allow refunds or exchanges, except warranty returns or as provided by state or federal law.

6. **Warranty.**

   6.1. **Limited Warranty.** Axon warrants that Axon-manufactured Devices, except for TASER devices covered under the TASER Appendix, are free from defects in workmanship and materials for one (1) year from the date of Customer's receipt, except Signal Sidearm which Axon warrants for thirty (30) months from Customer's receipt and Axon-manufactured accessories, which Axon warrants for ninety (90) days from Customer's receipt, respectively, from the date of Customer's receipt. Extended warranties run from the expiration of the one- (1-) year hardware warranty through the extended warranty term purchased.

   6.2. **Disclaimer. All software and Axon Cloud Services are provided "AS IS," without any warranty of any kind, either express or implied, including without limitation the implied warranties of merchantability, fitness for a particular purpose and non-infringement. Axon Devices and Services that are not manufactured, published or performed by Axon ("Third-Party Products") are not covered by Axon's warranty and are only subject to the warranties of the third-party provider or manufacturer. If Customer purchases Axon Loki, Customer acknowledges the Loki device is designed for operation in enclosed, controlled environments and must be used in compliance with all applicable laws and safety guidelines. Operation in open or unapproved areas may result in signal interference, loss of control, or damage, and Axon assumes no liability for improper use, including any resulting harm or regulatory violations.**

   6.3. **Claims.** If Axon receives a valid warranty claim for an Axon-manufactured Device during the warranty term, Axon's sole responsibility is to repair or replace the Axon-manufactured Device with the same or like Axon-manufactured Device, at Axon's option. A replacement Axon-manufactured Device will be new or like new.

Axon will warrant the replacement Axon-manufactured Device for the longer of (a) the remaining warranty of the original Axon-manufactured Device or (b) ninety (90) days from the date of repair or replacement.

6.3.1. If Customer exchanges an Axon Device or part, the replacement item becomes Customer's property, and the replaced item becomes Axon's property. Before delivering an Axon-manufactured Device for service, Customer must upload Axon-manufactured Device data to Axon Evidence or download it and retain a copy. Axon is not responsible for any loss of software, data, or other information contained in storage media or any part of the Axon-manufactured Device sent to Axon for service.

6.4. **Spare Axon Devices.** At Axon's reasonable discretion, Axon may provide Customer a predetermined number of spare Axon Devices as detailed in the Quote ("**Spare Axon Devices**"). Spare Axon Devices are intended to replace broken or non-functioning units while Customer submits the broken or non-functioning units, through Axon's warranty return process. Axon will repair or replace the unit with a replacement Axon Device. Title and risk of loss for all Spare Axon Devices shall pass to Customer in accordance with shipping terms of this Agreement. Axon assumes no liability or obligation in the event Customer does not utilize Spare Axon Devices for the intended purpose.

6.5. **Limitations.** Axon's warranty excludes damage related to: (a) failure to follow Axon Device use instructions; (b) Axon Devices used with equipment not manufactured or recommended by Axon; (c) abuse, misuse, or intentional damage to Axon Device; (d) force majeure; (e) Axon Devices repaired or modified by persons other than Axon without Axon's written permission; or (f) Axon Devices with a defaced or removed serial number. Axon's warranty will be void if Customer resells Axon Devices.

6.5.1. **To the extent permitted by law, the above warranties and remedies are exclusive. Axon disclaims all other warranties, remedies, and conditions, whether oral, written, statutory, or implied. If statutory or implied warranties cannot be lawfully disclaimed, then such warranties are limited to the duration of the warranty described above and by the provisions in this Agreement. Customer confirms and agrees that, in deciding whether to sign this Agreement, Customer has not relied on any statement or representation by Axon or anyone acting on behalf of Axon related to the subject matter of this Agreement that is not in this Agreement.**

6.6. **Online Support Platforms.** Use of Axon's online support platforms (e.g., Axon Academy and MyAxon) is governed by the Axon Online Support Platforms Terms of Use Appendix available at www.axon.com/sales-terms-and-conditions.

6.7. **Third-Party Hardware, Software and Services.** Use of hardware, software, or services other than those provided by Axon is governed by the terms, if any, entered into between Customer and the respective third-party provider, including, without limitation, the terms applicable to such software or services located at www.axon.com/sales-terms-and-conditions, if any.

6.8. **Axon Aid.** Upon mutual agreement between Axon and Customer, Axon may provide certain products and services to Customer, as a charitable donation under the Axon Aid program. In such event, Customer expressly waives and releases any and all claims, now known or hereafter known, against Axon and its officers, directors, employees, agents, contractors, affiliates, successors, and assigns (collectively, "**Releasees**"), including but not limited to, on account of injury, death, property damage, or loss of data, arising out of or attributable to the Axon Aid program whether arising out of the negligence of any Releasees or otherwise. Customer agrees not to make or bring any such claim against any Release, and forever release and discharge all Releasees from liability under such claims. Customer expressly allows Axon to publicly announce its participation in Axon Aid and use its name in marketing materials. Axon may terminate the Axon Aid program without cause immediately upon notice to the Customer.

7. **Free Trial.**

7.1. **Trial Period and License.** At any time during the Term, Customer and Axon may elect to enter a free trial of Axon Devices and Services new to the Customer for a designated period ("**Trial Period**") as described in a quote issued ("**Trial Quote**"). During the Trial Period, Axon grants Customer a nonexclusive, terminable, non-transferable, license to use new Axon Devices and Services provided for trial to the Customer ("**Trial Products**"). Trial Products may include Axon beta software or firmware which additional terms may be required and included within the Trial Quote. Axon may limit the number of Trial Products Customer receives within the Trial Quote. Axon may supply refurbished Trial Products. ALL FREE TRIAL PRODUCTS INCLUDING, WITHOUT LIMITATION, AXON CLOUD SERVICES, ARE PROVIDED "AS IS" AND TO THE EXTENT NOT PROHIBITED BY LAW, AXON DISCLAIMS ALL LIABILITY REGARDLESS OF THE CLAIM.

7.2. **Trial Quote Termination.** Upon at least 10 business days' prior written notice to Axon at any time prior to the end of the Trial Period, Customer may as its sole option, terminate the free Trial Period and underlying Trial Quote associated with the Trial Products for convenience. Customer's rights to the Trial Products will immediately terminate at the end of the Trial Period, and Customer will return any Trial Products hardware to

Axon within 10 days after the effective date of such termination or at the end of the Trial Period, excluding used CEW cartridges. If any individual component of the Trial Products is not returned, Axon will invoice Customer the MSRP of the unreturned items. Customer agrees to pay the invoice along with any applicable taxes and shipping. Customer will return the Trial Products to Axon in good working condition, minus normal wear and tear. Axon may charge Customer if there is damage beyond normal wear and tear. Any Customer Content shall be stored and returned pursuant to the Axon Cloud Services Terms of Use Appendix

8. **Statement of Work.** Certain Axon Devices and Services, including, but not limited to, Axon Interview Room, Axon Channel Services, Axon Justice Implementation, FUSUS, and Axon Fleet, may require a Statement of Work that details Axon's Service deliverables ("**SOW**"). In the event Axon provides an SOW to Customer, Axon is only responsible for the performance of Services described in the SOW. Additional services outside of the SOW, Quote, or this Agreement are out of scope. The Parties must document scope changes in a written and signed change order. Changes may require an equitable adjustment in fees or schedule. Any applicable SOW is incorporated into this Agreement by reference.

9. **Axon Device Warnings.** See www.axon.com/legal for the most current Axon Device warnings.

10. **Design Changes.** Axon may make design or feature changes to any Axon Device or Service without notifying Customer or making the same change to Axon Devices and Services previously purchased by Customer.

11. **Combined Offerings.** Some offerings in a Quote combine existing and pre-released Axon Devices or Services. Some offerings may not be available at the time of Customer's purchase. Axon will not provide a refund, credit, or additional discount beyond what is in the Quote due to delay of availability or Customer's choice not to utilize any portion of a combined offering.

12. **IP Rights.** Axon owns and reserves all right, title, and interest in Axon-manufactured Devices and Services and suggestions to Axon, including all related intellectual property rights. Customer will not cause any Axon proprietary rights to be violated.

13. **Customer Responsibilities.** Customer is responsible for (a) Customer's use of Axon Devices; (b) Customer or a Customer-authorized user's breach of this Agreement or violation of applicable law; (c) disputes between Customer and a third-party over Customer's use of Axon Devices; (d) secure and sustainable destruction and disposal of Axon Devices at Customer's cost; and (e) any regulatory violations or fines, as a result of improper destruction or disposal of Axon Devices.

14. **Termination.**

    14.1. **Effect of Termination**. Upon termination of this Agreement, Customer rights immediately terminate. Customer remains responsible for all fees incurred before the effective date of termination. If Customer purchases Axon Devices for less than the manufacturer's suggested retail price ("**MSRP**") and this Agreement terminates before the end of the Term, Axon will invoice Customer the difference between the MSRP for Axon Devices procured, including any Spare Axon Devices, and amounts paid towards those Axon Devices. Only if terminating for non-appropriation, Customer may return Axon Devices to Axon within thirty (30) days of termination. MSRP is the standalone price of the individual Axon Device at the time of sale. For multiple Axon Devices that may be combined as a single offering on a Quote, MSRP is the standalone price of all individual components.

15. **General.**

    15.1. **Compliance with Laws.** Each Party will comply with all applicable federal, state, and local laws, including without limitation, import and export control laws and regulations as well as firearm regulations and the Gun Control Act of 1968. Customer acknowledges that Axon Devices and Services are subject to U.S. and international export control laws, including the U.S. Export Administration Regulations (EAR) and International Traffic in Arms Regulations (ITAR). Customer represents and warrants that neither it nor any End User is a "Restricted Person," meaning any individual or entity that (1) is subject to U.S. sanctions or trade restrictions, (2) appears on any U.S. government restricted party list, (3) engages in prohibited weapons proliferation activities, or (4) is owned or controlled by, or acting on behalf of, such persons or entities. Customer must promptly notify Axon of any change in status, and Axon may terminate this Agreement if Customer or any End User becomes a Restricted Person or violates export laws.

    15.2. **Waiver.** No waiver or delay by either Party in exercising any right under this Agreement constitutes a waiver of that right.

    15.3. **Severability.** If a court of competent jurisdiction holds any portion of this Agreement invalid or unenforceable, the remaining portions of this Agreement will remain in effect.

Axon Cloud Services Terms of Use Appendix

1. **Definitions.**
   1.1. "**Data Controller**" means the natural or legal person, public authority, or any other body which alone or jointly with others determines the purposes and means of the processing of Personal Data.
   1.2. "**Data Processor**" means a natural or legal person, public authority or any other body which processes Personal Data on behalf of the Data Controller.
   1.3. "**Customer Content**" is data uploaded into, ingested by, or created in Axon Cloud Services within Customer's tenant, including media or multimedia uploaded into Axon Cloud Services by Customer. Customer Content includes Evidence but excludes Non-Content Data.
   1.4. "**Evidence**" is media or multimedia uploaded into Axon Evidence as 'evidence' by Customer. Evidence is a subset of Customer Content.
   1.5. "**End User**" means the natural person subject to Customer's authorized license grant who ultimately uses the Cloud Services as provided under this Agreement. End Users must adhere to the terms of use and are subject to any usage restrictions or limitations specified in this Agreement.
   1.6. "**Non-Content Data**" is data, configuration, and usage information about Customer's Axon Cloud Services tenant, Axon Devices and client software, and users that is transmitted or generated when using Axon Devices. Non-Content Data includes data about users captured during account management and customer support activities. Non-Content Data does not include Customer Content.
   1.7. "**Personal Data**" means any information relating to an identified or identifiable natural person. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
   1.8. "**Provided Data**" means de-identified, de-personalized, data derived from Customer's TASER energy weapon deployment reports, related TASER energy weapon logs, body-worn camera footage, and incident reports.
   1.9. "**Subprocessor**" means any third party engaged by the Data Processor to assist in data processing activities that the Data Processor is carrying out on behalf of the Data Controller.
   1.10. "**Transformed Data**" means the Provided Data used for the purpose of quantitative evaluation of the performance and effectiveness of TASER energy weapons in the field across a variety of circumstances.
2. **Access.** Upon Axon granting Customer a subscription to Axon Cloud Services, Customer may access and use Axon Cloud Services to store and manage Customer Content. Customer may not exceed the total number of End Users specified in the Quote. Axon Air requires an Axon Evidence subscription for each drone operator. For Axon Evidence access granted solely for TASER, Customer may access and use Axon Evidence only to store and manage TASER CEW data ("TASER Data") and Customer may not upload non-TASER Data to Axon Evidence.
3. **Customer Owns Customer Content.** Customer controls and owns all rights, title, and interest in Customer Content. Except as outlined herein, Axon obtains no interest in Customer Content, and Customer Content is not Axon's business records. Customer is solely responsible for uploading, sharing, managing, and deleting Customer Content. Axon will only have access to Customer Content for the limited purposes set forth herein. Customer agrees to allow Axon access to Customer Content to (a) perform troubleshooting, maintenance, or diagnostic screenings; and (b) enforce this Agreement or policies governing use of the Axon products.
4. **Security.** Axon will implement commercially reasonable and appropriate measures to secure Customer Content against accidental or unlawful loss, access or disclosure. Axon will maintain a comprehensive information security program to protect Axon Cloud Services and Customer Content including logical, physical access, vulnerability, risk, and configuration management; incident monitoring and response; encryption of uploaded digital evidence; security education; and data protection. Axon agrees to the Federal Bureau of Investigation Criminal Justice Information Services Security Addendum for its digital evidence or records management systems.
5. **Customer Responsibilities.** Customer is responsible for (a) ensuring Customer owns Customer Content or has the necessary rights to use Customer Content (b) ensuring no Customer Content or Customer End User's use

of Customer Content or Axon Cloud Services violates this Agreement or applicable laws; (c) maintaining necessary computer equipment and Internet connections for use of Axon Cloud Services and (d) verify the accuracy of any auto generated or AI-generated reports. If Customer becomes aware of any violation of this Agreement by an End User, Customer will immediately terminate that End User's access to Axon Cloud Services.

5.1. Customer will also maintain the security of End User usernames and passwords and security and access by end users to Customer Content. Customer is responsible for ensuring the configuration and utilization of Axon Cloud Services meet applicable Customer regulation and standards. Customer may not sell, transfer, or sublicense access to any other entity or person. If Customer provides access to unauthorized third-parties, Axon may assess additional fees along with suspending Customer's access. Customer shall contact Axon immediately if an unauthorized party may be using Customer's account or Customer Content, or if account information is lost or stolen.

5.2. To the extent Customer uses the Axon Cloud Services to interact with YouTube®, such use may be governed by the YouTube Terms of Service, available at https://www.youtube.com/static?template=terms.

6. **Privacy.** Customer's use of Axon Cloud Services is subject to the Axon Cloud Services Privacy Policy, a current version of which is available at https://www.axon.com/legal/cloud-services-privacy-policy. Customer agrees to allow Axon access to Non-Content Data from Customer to (a) perform troubleshooting, maintenance, or diagnostic screenings; (b) provide, develop, improve, and support current and future Axon products and related services; and (c) enforce this Agreement or policies governing the use of Axon products.

7. **Storage.** For Axon Unlimited Device Storage subscriptions, Customer may store unlimited data in Customer's Axon Evidence account only if the Axon Device data is shared to Customer through Axon Evidence from a partner agency using Axon Evidence, or the data originates from Axon Capture or an Axon Device. Axon may charge Customer additional fees for exceeding purchased storage amounts. Axon may place Customer Content that Customer has not viewed or accessed for six (6) months into archival storage. Customer Content in archival storage will not have immediate availability and may take up to twenty-four (24) hours to access.

7.1. **Third-Party Unlimited Storage.** For Third-Party Unlimited Storage the following restrictions apply: (i) it may only be used in conjunction with a valid Axon Evidence user license; (ii) is limited to data of the law enforcement Customer that purchased the Third-Party Unlimited Storage and the Axon Evidence End User; (iii) Customer is prohibited from storing data for other customers or law enforcement agencies; and (iv) Customer may only upload and store data that is directly related to (1) the investigation of, or the prosecution or defense of a crime, (2) common law enforcement activities, or (3) any Customer Content created by Axon Devices or Axon Evidence.

7.2. **Location of Storage.** Axon may transfer Customer Content to third-party subcontractors for storage. Axon will determine the locations of data centers for storage of Customer Content If Customer is located in the United States, Canada, or Australia, Axon will ensure all Customer Content stored in Axon Cloud Services remains in the country where Customer is located Ownership of Customer Content remains with Customer.

8. **Suspension.** Axon may temporarily suspend Customer's or any End User's right to access or use any portion or all of Axon Cloud Services immediately upon notice, if Customer or End User's use of or registration for Axon Cloud Services may (a) pose a security risk to Axon Cloud Services or any third-party; (b) adversely impact Axon Cloud Services, the systems, or content of any other customer; (c) subject Axon, Axon's affiliates, or any third-party to liability; or (d) be fraudulent. Customer remains responsible for all fees incurred through suspension. Axon will not delete Customer Content because of suspension, except as specified in this Agreement**.**

9. **Axon Cloud Services Warranty.** Axon disclaims any warranties or responsibility for data corruption or errors before Customer uploads data to Axon Cloud Services Service Offerings will be subject to the Axon Cloud Services Service Level Agreement, a current version of which is available at https://www.axon.com/products/axon-evidence/sla.

10. **Roles of the Parties.** To the extent that Customer is the Data Controller of Personal Data, Axon is its Data Processor. To the extent that Customer is a Data Processor of Personal Data, Axon is its Subprocessor. Notwithstanding the foregoing, to the extent any usage data (including query logs and metadata) and/or operations data (including billing and support data) in connection with Customer's use of the Services (collectively "Usage and Operations Data") is considered Personal Data, Axon is an independent Data Controller and shall Process such data in accordance with the Agreement and applicable data protection laws to develop, improve, support, and operate its products and services. For the avoidance of doubt, Axon will not disclose any Usage and Operations Data that includes confidential information with a third party except (a) in accordance with the relevant confidentiality provisions in the Agreement, or (b) to the extent the Usage and Operations Data is,

in accordance with applicable data protection laws, anonymized, de-identified, and/or aggregated such that it can no longer directly or indirectly identify Customer or any particular individual.

11. **Axon Cloud Services Restrictions.** Customer and Customer End Users (including employees, contractors, agents, officers, volunteers, and directors), may not, or may not attempt to:

    11.1. copy, modify, tamper with, repair, or create derivative works of any part of Axon Cloud Services;

    11.2. reverse engineer, disassemble, or decompile Axon Cloud Services or apply any process to derive any source code included in Axon Cloud Services, or allow others to do the same;

    11.3. access or use Axon Cloud Services with the intent to gain unauthorized access, avoid incurring fees or exceeding usage limits or quotas;

    11.4. use trade secret information contained in Axon Cloud Services, except as expressly permitted in this Agreement;

    11.5. access Axon Cloud Services to build a competitive device or service or copy any features, functions, or graphics of Axon Cloud Services;

    11.6. remove, alter, or obscure any confidentiality or proprietary rights notices (including copyright and trademark notices) of Axon's or Axon's licensors on or within Axon Cloud Services; or

    11.7. use Axon Cloud Services to store or transmit infringing, libelous, or other unlawful or tortious material; material in violation of third-party privacy rights; or malicious code.

12. **After Termination.** Axon will not delete Customer Content for ninety (90) days following termination. Axon Cloud Services will not be functional during these ninety (90) days other than the ability to retrieve Customer Content. Customer will not incur additional fees if Customer downloads Customer Content from Axon Cloud Services during this time. Axon has no obligation to maintain or provide Customer Content after these ninety (90) days and will thereafter, unless legally prohibited, delete all Customer Content. Upon request, Axon will provide written proof that Axon successfully deleted and fully removed all Customer Content from Axon Cloud Services.

13. **Post-Termination Assistance.** Axon will provide Customer with the same post-termination data retrieval assistance that Axon generally makes available to all customers. Requests for Axon to provide additional assistance in downloading or transferring Customer Content, including requests for Axon's data egress service, will result in additional fees and Axon will not warrant or guarantee data integrity or readability in the external system.

14. **U.S. Government Rights.** If Customer is a U.S. Federal department or using Axon Cloud Services on behalf of a U.S. Federal department, Axon Cloud Services is provided as a "commercial item," "commercial computer software," "commercial computer software documentation," and "technical data", as defined in the Federal Acquisition Regulation and Defense Federal Acquisition Regulation Supplement. If Customer is using Axon Cloud 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 use of Axon Cloud Services.

15. **Survival.** Upon any termination of this Agreement, the following sections in this Appendix will survive: Customer Owns Customer Content, Privacy, Storage, Axon Cloud Services Warranty, Customer Responsibilities and Axon Cloud Services Restrictions.

Axon Customer Experience Improvement Program Appendix

The ACEIP is designed to accelerate Axon's development of technology, such as building and supporting automated features, aiming to increase safety within communities and efficiency in public safety. Axon may make limited use of Customer Content from participating customers to provide, develop, improve, and support current and future Axon products (collectively, "ACEIP Purposes"). ACEIP has 2 modes of participation, Basic and Custom. Customer is enrolled in ACEIP Basic by default. If Customer does not want to participate in ACEIP Basic, ACEIP Custom, or both, Customer can revoke its consent at any time via email to aceip@axon.com.

Axon Obligations

ACEIP Basic

When Axon uses Customer Content for ACEIP Purposes, Axon will:

- Use Customer Content only for ACEIP Purposes.
- Prohibit direct human access to Customer Content, including by Axon personnel and subprocessors, except as needed to perform or validate deletion.
- Retain Customer Content only as long as needed to create Transformed Content (defined below) and validate the transformations.
- Apply privacy-preserving transformations that remove identifying information appropriate to the use case ("Transformed Content"). AI model weights and similar insights that do not contain Customer Content are Transformed Content. Transformed Content is not Customer Content.
- Retain and permit direct human access to Transformed Content for ACEIP Purposes.
- Maintain security, privacy, and data governance programs as described in the Axon Cloud Services Terms Appendix, and apply them to ACEIP.

Transparency Portal Publication

Before activating a use case, Axon will publish it on the Axon Transparency Portal, including the product development purpose, data types involved, and privacy-preserving techniques used. Axon will also notify ACEIP participants when the Transparency Portal is updated with a new or materially changed use case. Fifteen (15) calendar days after notification, Axon may activate the use case for all Basic participants.

Opt Out

Customer may opt out of ACEIP Basic at any time via aceip@axon.com. Axon endeavors to implement opt outs within fifteen (15) calendar days. Transformations of Customer Content cease when Axon implements the opt out. Axon may retain Transformed Content created before it implemented the opt out request.

ACEIP Custom

Custom use cases may be governed by separate written terms between Axon and Customer. Those terms will control that use case. Please direct inquiries regarding Custom participation to aceip@axon.com.

Axon ALPR Appendix

If Axon Fleet 2, Axon Fleet 3, or any future generation of Axon Fleet (collectively, "**Axon Fleet**") or Axon Outpost or Axon Lightpost (collectively all "ALPR Products") is included on the Quote, this Appendix applies.

1. **Customer Responsibilities.**

   1.1. Customer must ensure its infrastructure and vehicles adhere to the minimum requirements to operate Axon ALPR Products as established by Axon during the qualifier call and on-site assessment at Customer and in any technical qualifying questions. If Customer's representations are inaccurate, the Quote is subject to change.

   1.2. Customer is responsible for providing a suitable work area for Axon or Axon third-party providers to install Axon ALPR Products into Customer vehicles and/or at designated installation location(s).s Customer is responsible for making available all vehicles for which installation services were purchased and preparing all installation sites, during the agreed upon onsite installation dates, Failure to make vehicles available or prepare installation sites may require an equitable adjustment in fees or schedule

2. **Third-party Installer.** Axon will not be liable for the failure of Axon Fleet, Axon Outpost, or Axon Lightpost hardware to operate per specifications if such failure results from installation not performed by, or as directed by Axon.

3. **Axon Fleet Specific Terms.**

   3.1. **Cradlepoint.** If Customer purchases Cradlepoint hardware, software, or services, Customer will comply with Cradlepoint's end user license agreement. The term of the Cradlepoint license may differ from the Axon Evidence Subscription. If Customer requires Cradlepoint support, Customer will contact Cradlepoint directly. By accepting a Quote including Cradlepoint products, Customer designates and authorizes Axon as its partner of record for purposes of Cradlepoint product renewals, support coordination, and other relevant functions. This designation applies to all Cradlepoint products acquired by Customer during the Subscription Term of the applicable Quote whether directly from Cradlepoint, through Axon, or through any third-party vendor or distributor. Axon shall have no liability to Customer or any third party arising out of or relating to Axon's acts or omissions as the Partner of Record. Customer has the right to opt out of this authorization at any time by providing prior written notification to both Axon and Cradlepoint. Upon such notification, the designation will be removed. This authorization remains effective until formally removed in accordance with this section or as otherwise agreed between the parties in the Agreement.

   3.2. **Axon Vehicle Software License.** Axon grants Customer a non-exclusive, royalty-free, worldwide, perpetual license to use ViewXL or Dashboard (collectively, "Axon Vehicle Software".) "Use" means storing, loading, installing, or executing Axon Vehicle Software solely for data communication with Axon Devices. The Axon Vehicle Software term begins upon the start of the Axon Evidence Subscription

   3.3. **Restrictions.** Customer may not: (a) modify, alter, tamper with, repair, or create derivative works of Axon Vehicle Software; (b) reverse engineer, disassemble, or decompile Axon Vehicle Software, apply any process to derive the source code of Axon Vehicle Software, or allow others to do so; (c) access or use Axon Vehicle Software to avoid incurring fees or exceeding usage limits; (d) copy Axon Vehicle Software in whole or part; (e) use trade secret information contained in Axon Vehicle Software; (f) resell, rent, loan or sublicense Axon Vehicle Software; (g) access Axon Vehicle Software to build a competitive device or service or copy any features, functions or graphics of Axon Vehicle Software; or (h) remove, alter or obscure any confidentiality or proprietary rights notices (including copyright and trademark notices) of Axon or Axon's licensors on or within Axon Vehicle Software.

   16. **Axon Outpost Specific Terms.**

   3.4. **Outpost License and Permits**. Customers will obtain, maintain all legally required permits, authorizations, and/or licensing in order to place, maintain, and/or remove the Axon Outpost device at the installation location including licenses or permits for fixed installation of poles. If mutually agreed by the parties, Axon or an Axon authorized subcontractor may assist with obtaining the necessary local, state, or Federal approvals before installing Axon Outpost.

   17. **Installation. Customer will adhere to the installation requirements as agreed in the Outpost SOW.**

   18. **Vandalism or Motor Vehicle Accident Warranty. If Customer purchases the Vandalism and Accident warranty, Axon will provide up to two (2) replacements per warranty purchased if your Outpost is damaged due to vandalism or a motor vehicle accident. Axon will make a commercially reasonable effort**

to provide new installation free of charge, but installation may require additional cost. Axon does not provide refunds or credits if the warranty is not used during the Term of the Quote.

19. **Axon Lightpost Specific Terms.**

3.5. **Ubicquia.** If Customer purchases Lightpost hardware and installation services, any warranties for the hardware are provided exclusively by the third-party manufacturer Ubicquia. All hardware-related support or warranty claims must be directed to the respective third-party provider. Axon is not responsible for servicing or replacing hardware. Axon will provide and support software components in accordance with the applicable Quote.

3.6. **Installation.** Installation of Axon Lightpost equipment will be performed by a third-party service provider authorized by Axon. Axon does not directly perform installation services.

3.7. **Power.** Customer agrees to supply a power source, in compliance with Lightpost requirements, at each site where a Lightpost device is installed. The power must be available on a 24-hour, 7 days per week (24/7) basis.

20. **Wireless Offload Server**

7.1 **License Grant.** Axon grants Customer a non-exclusive, royalty-free, worldwide, perpetual license to use Wireless Offload Server ("**WOS**"). "Use" means storing, loading, installing, or executing WOS solely for data communication with Axon Devices for the number of licenses purchased. The WOS term begins upon the start of the Axon Evidence Subscription.

7.2 **Restrictions.** Customer may not: (a) modify, alter, tamper with, repair, or create derivative works of WOS; (b) reverse engineer, disassemble, or decompile WOS, apply any process to derive the source code of WOS, or allow others to do so; (c) access or use WOS to avoid incurring fees or exceeding usage limits; (d) copy WOS in whole or part; (e) use trade secret information contained in WOS; (f) resell, rent, loan or sublicense WOS; (g) access WOS to build a competitive device or service or copy any features, functions or graphics of WOS; or (h) remove, alter or obscure any confidentiality or proprietary rights notices (including copyright and trademark notices) of Axon or Axon's licensors on or within WOS.

7.3 **Updates.** If Customer purchases WOS maintenance, Axon will make updates and error corrections to WOS ("**WOS Updates**") available electronically via the Internet or media as determined by Axon. Customer is responsible for establishing and maintaining adequate Internet access to receive WOS Updates and maintaining computer equipment necessary for use of WOS. The Quote will detail the maintenance term.

7.4 **WOS Support.** Upon request by Axon, Customer will provide Axon with access to Customer's store and forward servers solely for troubleshooting and maintenance.

21. **Acceptance Checklist. If Axon provides Services to Customer pursuant to any statement of work in connection with Axon ALPR Products, within seven (7) days of the date on which Customer retrieves Customer's vehicle(s) from the Axon installer or Axon Outpost or Axon Lightpost installation is complete, said ALPR Products having been installed and configured with tested and fully and properly operational hardware and software identified above, Customer will receive a Professional Services Acceptance Checklist to submit to Axon indicating acceptance or denial of said deliverables. In the event Customer does not respond to the Professional Services Acceptance Checklist within seven (7) business days, the installation of the ALPR Products and services shall be deemed accepted.**

Axon Application Programming Interface Appendix

This Appendix applies if Axon's API Services or a subscription to Axon Cloud Services are included on the Quote.

1. **Definitions.**

   1.1. "**API Client**" means the software that acts as the interface between Customer's computer and the server, which is already developed or to be developed by Customer.

   1.2. "**API Interface**" means software implemented by Customer to configure Customer's independent API Client Software to operate in conjunction with the API Service for Customer's authorized Use.

   1.3. "**Axon Evidence Partner API, API or Axon API**" (collectively "**API Service**") means Axon's API which provides a programmatic means to access data in Customer's Axon Evidence account or integrate Customer's Axon Evidence account with other systems.

   1.4. "**Use**" means any operation on Customer's data enabled by the supported API functionality.

2. **Purpose and License.**

   2.1. Customer may use API Service and data made available through API Service, in connection with an API Client developed by Customer. Axon may monitor Customer's use of API Service to ensure quality, improve Axon devices and services, and verify compliance with this Agreement. Customer agrees to not interfere with such monitoring or obscure from Axon Customer's use of API Service. Customer will not use API Service for commercial use.

   2.2. Axon grants Customer a non-exclusive, non-transferable, non-sublicensable, worldwide, revocable right and license during the Term to use API Service, solely for Customer's Use in connection with Customer's API Client.

   2.3. Axon reserves the right to set limitations on Customer's use of the API Service, such as a quota on operations, to ensure stability and availability of Axon's API. Axon will use reasonable efforts to accommodate use beyond the designated limits.

3. **Configuration.** Customer will work independently to configure Customer's API Client with API Service for Customer's applicable Use. Customer will be required to provide certain information (such as identification or contact details) as part of the registration. Registration information provided to Axon must be accurate. Customer will inform Axon promptly of any updates. Upon Customer's registration, Axon will provide documentation outlining API Service information.

4. **Customer Responsibilities.** When using API Service, Customer and its End Users shall not:

   4.1. use API Service in any way other than as expressly permitted under this Agreement;

   4.2. use in any way that results in, or could result in, any security breach to Axon;

   4.3. perform an action with the intent of introducing any virus, worm, defect, Trojan horse, malware, or any item of a destructive nature to Axon Devices and Services;

   4.4. interfere with, modify, disrupt or disable features or functionality of API Service or the servers or networks providing API Service;

   4.5. reverse engineer, decompile, disassemble, or translate or attempt to extract the source code from API Service or any related software;

   4.6. create an API Interface that functions substantially the same as API Service and offer it for use by third parties;

   4.7. provide use of API Service on a service bureau, rental or managed services basis or permit other individuals or entities to create links to API Service;

   4.8. frame or mirror API Service on any other server, or wireless or Internet-based device;

   4.9. make available to a third-party, any token, key, password or other login credentials to API Service;

   4.10. take any action or inaction resulting in illegal, unauthorized or improper purposes; or

   4.11. disclose Axon's API manual.

5. **API Content.** All content related to API Service, other than Customer Content or Customer's API Client content, is

considered Axon's API Content, including:

5.1. the design, structure and naming of API Service fields in all responses and requests;

5.2. the resources available within API Service for which Customer takes actions on, such as evidence, cases, users, or reports;

5.3. the structure of and relationship of API Service resources; and

5.4. the design of API Service, in any part or as a whole.

6. **Prohibitions on API Content.** Neither Customer nor its End Users will use API content returned from the API Interface to:

6.1. scrape, build databases, or otherwise create permanent copies of such content, or keep cached copies longer than permitted by the cache header;

6.2. copy, translate, modify, create a derivative work of, sell, lease, lend, convey, distribute, publicly display, or sublicense to any third-party;

6.3. misrepresent the source or ownership; or

6.4. remove, alter, or obscure any confidentiality or proprietary rights notices (including copyright and trademark notices).

7. **API Updates.** Axon may update or modify the API Service from time to time ("**API Update**"). Customer is required to implement and use the most current version of API Service and to make any applicable changes to Customer's API Client required as a result of such API Update. API Updates may adversely affect how Customer's API Client access or communicate with API Service or the API Interface. Each API Client must contain means for Customer to update API Client to the most current version of API Service. Axon will provide support for one (1) year following the release of an API Update for all depreciated API Service versions.

Axon Event Offer Appendix

If the Agreement includes the provision of, or Axon otherwise offers, ticket(s), travel and/or accommodation for select events hosted by Axon ("Axon Event"), the following shall apply:

1. **General.** Subject to the terms and conditions specified below and those in the Agreement, Axon may provide Customer with one or more offers to fund Axon Event ticket(s), travel and/or accommodation for Customer-selected employee(s) to attend one or more Axon Events. By entering into the Agreement, Customer warrants that it is appropriate and permissible for Customer to receive the referenced Axon Event offer(s) based on Customer's understanding of the terms and conditions outlined in this Axon Event Offer Appendix.
2. **Attendee/Employee Selection.** Customer shall have sole and absolute discretion to select the Customer employee(s) eligible to receive the ticket(s), travel and/or accommodation that is the subject of any Axon Event offer(s).
3. **Compliance.** It is the intent of Axon that any and all Axon Event offers comply with all applicable laws, regulations and ethics rules regarding contributions, including gifts and donations. Axon's provision of ticket(s), travel and/or accommodation for the applicable Axon Event to Customer is intended for the use and benefit of Customer in furtherance of its goals, and not the personal use or benefit of any official or employee of Customer. Axon makes this offer without seeking promises or favoritism for Axon in any bidding arrangements. Further, no exclusivity will be expected by either party in consideration for the offer. Axon makes the offer with the understanding that it will not, as a result of such offer, be prohibited from any procurement opportunities or be subject to any reporting requirements. If Customer's local jurisdiction requires Customer to report or disclose the fair market value of the benefits provided by Axon, Customer shall promptly contact Axon to obtain such information, and Axon shall provide the information necessary to facilitate Customer's compliance with such reporting requirements.
4. **Assignability.** Customer may not sell, transfer, or assign Axon Event ticket(s), travel and/or accommodation provided under the Agreement.
5. **Availability.** The provision of all offers of Axon Event ticket(s), travel and/or accommodation is subject to availability of funds and resources. Axon has no obligation to provide Axon Event ticket(s), travel and/or accommodation.
6. **Revocation of Offer.** Axon reserves the right at any time to rescind the offer of Axon Event ticket(s), travel and/or accommodation to Customer if Customer or its selected employees fail to meet the prescribed conditions or if changes in circumstances render the provision of such benefits impractical, inadvisable, or in violation of any applicable laws, regulations, and ethics rules regarding contributions, including gifts and donations.