REFERENCE AGREEMENT FOR PROFESSIONAL SERVICES

DIGITAL EVIDENCE MANAGEMENT SYSTEM

BETWEEN

COOK COUNTY GOVERNMENT

COOK COUNTY STATES ATTORNEY'S OFFICE

AND

AXON ENTERPRISE INC

CONTRACT NO. 2526-10211
PURCHASE ORDER NO. 70000385282

UNIVERSITY OF NEBRASKA MASTER AGREEMENT #3544-21-4615

NON-FEDERALLY FUNDED CONTRACT

PROFESSIONAL SERVICES AGREEMENT

TABLE OF CONTENTS

List of Exhibits

Attachments

AGREEMENT

This Agreement is made and entered into by and between the County of Cook, a public body corporate of the State of Illinois, on behalf of Office of the Chief Procurement Officer hereinafter referred to as "County" and Axon Enterprise, Inc. , doing business as a (an) corporation of the State of Arizona hereinafter referred to as "Consultant", pursuant to authorization by the Cook County Board of Commissioners on December 18, 2025, as evidenced by Board Authorization letter attached hereto as EXHIBIT "8".

BACKGROUND

Whereas, the County, pursuant to Section 34-140 (the "Reference Contract Ordinance") of the Cook County Procurement Code, states: "If a governmental agency has awarded a contract through a competitive method for the same or similar supplies, equipment, goods or services as that sought by the County, the Procurement may be made from that vendor at a price or rate at least as favorable as that obtained by that government agency without utilizing a competitive procurement method set forth in this Procurement Code;" and

Whereas, the University of Nebraska in conjunction with OMNIA Partners, solicited a formal Request for Proposal process for Body Worn Cameras and Related Products, which Related Products included Digital Evidence Storage and Digital Evidence Management Services and the Consultant was identified as the qualified and best value provider for the services; and

Whereas, the University of Nebraska entered into a contract on December 21, 2022 for the provision of services by the Consultant for the University of Nebraska relative to Digital Evidence Storage and Digital Evidence Management, a copy of the contract is attached hereto as Attachment 1 for reference purposes only, but the terms of the University of Nebraska are not made a part of or incorporated into this Agreement; and

Whereas, the County wishes to leverage the procurement efforts of the University of Nebraska; and

Whereas, the County, through the Office of States Attorney desires certain similar services of the Consultant; and

Whereas, County Offices, Departments, and Agencies may utilize this Agreement for specific contracted procurement efforts; and

Whereas, the Consultant agrees to provide Digital Evidence Storage and Digital Evidence Management, incorporated as Exhibit 1; and

Whereas, the Consultant warrants that it is ready, willing and able to deliver these services set forth in Exhibit 1, all on pricing and payment terms equivalent to or more favorable to the County than those contained in the University of Nebraska Master Agreement #3544-21-4615.

NOW, THEREFORE, the County and Consultant agree as follows:

TERMS AND CONDITIONS

ARTICLE 1) INCORPORATION OF BACKGROUND

The Background information set forth above is incorporated by reference as if fully set forth here.

ARTICLE 2) DEFINITIONS

a) Definitions

The following words and phrases have the following meanings for purposes of this Agreement:

"**Additional Services**" means those services which are within the general scope of Services of this Agreement, but beyond the description of services required under Article 3, and all services reasonably necessary to complete the Additional Services to the standards of performance required by this Agreement. Any Additional Services requested by the Using Agency require the approval of the Chief Procurement Officer in a written amendment to this Agreement before Consultant is obligated to perform those Additional Services and before the County becomes obligated to pay for those Additional Services.

"**Agreement**" means this Professional Services Agreement, including all exhibits attached to it and incorporated in it by reference, and all amendments, modifications or revisions made in accordance with its terms.

"**Chief Procurement Officer**" means the Chief Procurement Officer for the County of Cook and any representative duly authorized in writing to act on his behalf.

"**Services**" means, collectively, the services, duties and responsibilities described in Article 3 of this Agreement and any and all work necessary to complete them or carry them out fully and to the standard of performance required in this Agreement.

"**Subcontractor**" or **"Subconsultant"** means any person or entity with whom Consultant contracts to provide any part of the Services, of any tier, suppliers and materials providers, whether or not in privity with Consultant.

"Using Agency" shall mean the department of agency within Cook County including elected officials.

b) Interpretation

i) The term "**include**" (in all its forms) means "include, without limitation" unless the context clearly states otherwise.

ii) All references in this Agreement to Articles, Sections or Exhibits, unless otherwise expressed or indicated are to the Articles, Sections or Exhibits of this Agreement.

iii) Words importing persons include firms, associations, partnerships, trusts, corporations and other legal entities, including public bodies, as well as natural persons.

iv) Any headings preceding the text of the Articles and Sections of this Agreement, and any tables of contents or marginal notes appended to it are solely for convenience or reference and do not constitute a part of this Agreement, nor do they affect the meaning, construction or effect of this Agreement.

v) Words importing the singular include the plural and vice versa. Words of the masculine gender include the correlative words of the feminine and neuter genders.

vi) All references to a number of days mean calendar days, unless expressly indicated otherwise.

c) Incorporation of Exhibits

The following attached Exhibits are made a part of this Agreement:

Exhibit 1	Axon Quote Summary
Exhibit 2	Axon Online Support Platforms Terms of Use
Exhibit 3	Axon Master Services and Purchasing Agreement
Exhibit 4	Cook County Information Technology and Data Special Conditions (ITDSC)
Exhibit 5	CJIS Security Addendum
Exhibit 6	Minority and Women Owned Business Enterprise Commitment
Exhibit 7	Evidence of Insurance
Exhibit 8	Board Authorization
Exhibit 9	Identification of Subcontractors/Supplier/Subconsultant Form
Exhibit 10	Electronic Payables Program (“E-Payables”)
Exhibit 11	Economic Disclosure Statement

d) Order of Precedence

In the event there is a conflict between or among any of the documents specified in subsection (c) Incorporation of Exhibits, the terms of the Professional Services Agreement shall control. This Agreement shall be interpreted and construed based upon the following Order of Precedence. Such order of precedence shall govern to resolve all cases of conflict, ambiguity or inconsistency between Exhibits:

Exhibit 1	Axon Quote Summary
Exhibit 2	Axon Online Support Platforms Terms of Use
Exhibit 3	Axon Master Services and Purchasing Agreement

Exhibit 4	Cook County Information Technology and Data Special Conditions (ITDSC)
Exhibit 5	CJIS Security Addendum
Exhibit 6	Minority and Women Owned Business Enterprise Commitment
Exhibit 7	Evidence of Insurance
Exhibit 8	Board Authorization
Exhibit 9	Identification of Subcontractors/Supplier/Subconsultant Form
Exhibit 10	Electronic Payables Program ("E-Payables")
Exhibit 11	Economic Disclosure Statement

ARTICLE 3) DUTIES AND RESPONSIBILITIES OF CONSULTANT

a) Scope of Services

This description of Services is intended to be general in nature and is neither a complete description of Consultant's Services nor a limitation on the Services that Consultant is to provide under this Agreement. Consultant must provide the Services in accordance with the standards of performance set forth in Section 3c. The Services that Consultant must provide include, but are not limited to, those described in Exhibit 1, which is attached to this Agreement and incorporated by reference as if fully set forth here.

b) Deliverables

In carrying out its Services, Consultant must prepare or provide to the County various Deliverables. "**Deliverables**" include work product, such as written reviews, recommendations, reports and analyses, solely and exclusively created by Consultant for the County.

The County may reject Deliverables that do not include relevant information or data, or do not include all documents or other materials specified in this Agreement or reasonably necessary for the purpose for which the County made this Agreement or for which the County intends to use the Deliverables. If the County determines that Consultant has failed to comply with the foregoing standards, it has 30 days from the discovery to notify Consultant of its failure. If Consultant does not correct the failure, if it is possible to do so, within 30 days after receipt of notice from the County specifying the failure, then the County, by written notice, may treat the failure as a default of this Agreement under Article 9.

Partial or incomplete Deliverables may be accepted for review only when required for a specific and well-defined purpose and when consented to in advance by the County. Such Deliverables will not be considered as satisfying the requirements of this Agreement and partial or incomplete Deliverables in no way relieve Consultant of its commitments under this Agreement.

c) Standard of Performance

Consultant must perform all Services required of it under this Agreement with that degree of skill, care and diligence normally shown by a consultant performing services of a scope and purpose and magnitude comparable with the nature of the Services to be provided under this Agreement. Consultant acknowledges that it is entrusted with or has access to valuable and confidential information and records of the County and with respect to that information, Consultant agrees to be held to the standard of care of a fiduciary.

Consultant must assure that all Services that require the exercise of professional skills or judgment are accomplished by professionals qualified and competent in the applicable discipline and appropriately licensed, if required by law. Consultant must provide copies of any such licenses. Consultant remains responsible for the professional and technical accuracy of all Services or Deliverables furnished, whether by Consultant or its Subconsultants or others on its behalf. All Deliverables must be prepared in a form and content satisfactory to the Using Agency and delivered in a timely manner consistent with the requirements of this Agreement.

If Consultant fails to comply with the foregoing standards, Consultant must perform again, at its own expense, all Services required to be re-performed as a direct or indirect result of that failure. Any review, approval, acceptance or payment for any of the Services by the County does not relieve Consultant of its responsibility for the professional skill and care and technical accuracy of its Services and Deliverables. This provision in no way limits the County's rights against Consultant either under this Agreement, at law or in equity.

d) Personnel

i) **Adequate Staffing**

Consultant must, upon receiving a fully executed copy of this Agreement, assign and maintain during the term of this Agreement and any extension of it an adequate staff of competent personnel that is fully equipped, licensed as appropriate, available as needed, qualified and assigned exclusively to perform the Services. Consultant must include among its staff the Key Personnel and positions as identified below. The level of staffing may be revised from time to time by notice in writing from Consultant to the County and with written consent of the County, which consent the County will not withhold unreasonably. If the County fails to object to the revision within 14 days after receiving the notice, then the revision will be considered accepted by the County.

ii) **Key Personnel**

Consultant must not reassign or replace Key Personnel without the written consent of the County, which consent the County will not unreasonably withhold. "**Key Personnel**" means those job titles and the persons assigned to those positions in accordance with the provisions of this Section 3.d(ii). The Using Agency may at any time in writing notify Consultant that the County will no longer accept performance of Services under this Agreement by one or more Key Personnel listed. Upon that notice Consultant must immediately suspend the services of the key person or persons and must replace him or them in accordance with the terms of this Agreement. A list of Key Personnel is found in Exhibit 1.

iii) **Salaries and Wages**

Consultant and Subconsultants must pay all salaries and wages due all employees performing Services under this Agreement unconditionally and at least once a month without deduction or rebate on any account, except only for those payroll deductions that are mandatory by law or are permitted under applicable law and regulations. If in the performance of this Agreement Consultant underpays any such salaries or wages, the Comptroller for the County may withhold, out of payments due to Consultant, an amount sufficient to pay to employees underpaid the difference between the salaries or wages required to be paid under this Agreement and the salaries or wages actually paid these employees for the total number of hours worked. The amounts withheld may be disbursed by the Comptroller for and on account of Consultant to the respective employees to whom they are due. The parties acknowledge that this Section 3.d(iii) is solely for the benefit of the County and that it does not grant any third party beneficiary rights.

e) Minority and Women Owned Business Enterprises Commitment

In the performance of this Agreement, including the procurement and lease of materials or equipment, Consultant must abide by the minority and women's business enterprise commitment requirements of the Cook County Ordinance, (Article IV, Section 34-267 through 272) except to the extent waived by the Compliance Director, which are set forth in Exhibit 6. Consultant's completed MBE/WBE Utilization Plan evidencing its compliance with this requirement are a part of this Agreement, in Form 1 of the MBE/WBE Utilization Plan, upon acceptance by the Compliance Director. Consultant must utilize minority and women's business enterprises at the greater of the amounts committed to by the Consultant for this Agreement in accordance with Form 1 of the MBE/WBE Utilization Plan.

f) Insurance

Consultant must provide and maintain at Consultant's own expense, during the term of this Agreement and any time period following expiration if Consultant is required to return and perform any of the Services or Additional Services under this Agreement, the insurance coverages and requirements specified below, insuring all operations related to this Agreement.

i) **Insurance To Be Provided**

Insurance Requirements
The Consultant, at its cost, shall secure and maintain at all times, unless specified otherwise, until completion of the term of this Contract the insurance specified below.

Nothing contained in these insurance requirements is to be construed as limiting the extent of the
Consultant's responsibility for payment of damages resulting from its operations under this Contract.

The Consultant shall require all Subcontractors to provide the insurance required in this Contract, or Consultant may provide the coverages for Subcontractors. All Subcontractors are subject to the same insurance requirements as Consultant except paragraph (d) Excess/Umbrella Liability or unless specified otherwise.

The Cook County Department of Risk Management maintains the right to modify, delete, alter or change these requirements. Consultant shall have the opportunity to review any modified insurance requirement to ensure compliance.

Coverages

(a) **Workers Compensation Insurance**
Workers' Compensation shall be in accordance with the laws of the State of Illinois or any other applicable jurisdiction.

The Workers Compensation policy shall also include the following provisions:

Employers' Liability coverage with a limit of
$1,000,000 each Accident
$1,000,000 each Employee
$1,000,000 Policy Limit for Disease

(b) **Commercial General Liability Insurance**
The Commercial General Liability shall be on an occurrence form basis (ISO Form CG 0001 or equivalent) to cover bodily injury, personal injury and

property damage.

Each Occurrence	$1,000,000
General Aggregate	$1,000,000
Completed Operations Aggregate	$2,000,000

The General Liability policy shall include the following coverages:
(1) All premises and operations;
(2) Contractual Liability;
(3) Products/Completed Operations;
(4) Severability of interest/separation of insureds clause

(c) **Commercial Automobile Liability Insurance**
When any vehicles are used in the performance of this contract, Consultant shall secure Automobile Liability Insurance for bodily injury and property damage arising from the Ownership, maintenance or use of owned, hired, and non-owned vehicles with a limit no less than $1,000,000 per accident.

(d) **Excess/Umbrella Liability**
Such policy shall be excess over Commercial General Liability, Automobile Liability, and Employer's Liability with limits not less than the following amounts:

Each Occurrence: $1,000,000

(e) **Professional Liability (Errors & Omissions)**
The Consultant shall secure insurance appropriate to the Consultant's profession covering all claims arising out of the performance or nonperformance of professional services for the County under this Contract. This insurance shall remain in force for the life of the Consultant's obligations under this Contract and shall have a limit of liability of not less than $1,000,000 per claim.
If any such policy is written on a claims-made form:
(1) The retroactive coverage date shall be no later than the effective date of this contract.
(2) If coverage is canceled or non-renewed, and not replaced with another claims-made policy form with a retroactive date on or before this contract effective date, the Consultant must maintain "extended reporting" coverage for a minimum of three (3) year after completion of services.

(f) **Network Security & Privacy Liability (Cyber)**
The Consultant shall secure coverage for first and third-party claims with limits not less than $1,000,000 per occurrence or claim, $1,000,000 aggregate.
If any such policy is written on a claims-made form:
(1) The retroactive coverage date shall be no later than the effective date of this contract.

(2) If coverage is canceled or non-renewed, and not replaced with another claims-made policy form with a retroactive date on or before this contract effective date, the Consultant must maintain "extended reporting" coverage for a minimum of three (3) year after completion of services.

Additional requirements

(a) **Additional Insured**

The required insurance policies, with the exception of Workers Compensation and Errors & Omissions, shall name Cook County, its officials, employees, and agents as additional insureds with respect to operations performed on a primary and non-contributory basis. Any insurance or self-insurance maintained by Cook County shall be excess of the Consultant's insurance and shall not contribute with it. The full policy limits and scope of protection shall apply to Cook County as an additional insured even if they exceed the minimum insurance requirements specified herein.

All insurance companies providing coverage shall be licensed or approved by the Department of Insurance, State of Illinois, and shall have a financial rating no lower than (A-) VII as listed in A.M. Best's Key Rating Guide, current edition, or interim report. Companies with ratings lower than (A-) VII will be acceptable only upon consent of the Cook County Department of Risk Management. The insurance limits required herein may be satisfied by a combination of primary, umbrella and/or excess liability insurance policies.

(b) **Insurance Notices**

The Consultant shall provide the Office of the Chief Procurement Officer with thirty (30) days advance written notice in the event any required insurance will be cancelled, materially reduced or non-renewed. The Consultant shall secure replacement coverage to comply with the stated insurance requirements and provide new certificates of insurance to the Office of the Chief Procurement Officer.

Prior to the date on which the Consultant commences performance of its part of the work, the Consultant shall furnish to the Office of the Chief Procurement Officer certificates of insurance maintained by Consultant. The receipt of any certificate of insurance does not constitute Contract by the County that the insurance requirements have been fully met or that the insurance policies indicated on the certificate of insurance are in compliance with insurance required above.

In no event shall any failure of the County to receive certificates of insurance required hereof or to demand receipt of such Certificates of Insurance be construed as a waiver of the Consultant's obligations to obtain insurance pursuant to these insurance requirements.

(c) **Waiver of Subrogation Endorsements**
All insurance policies must contain a Waiver of Subrogation Endorsement in favor of Cook County.

g) Indemnification

The Consultant covenants and agrees to indemnify and save harmless the County and its commissioners, officials, employees, agents and representatives, and their respective heirs, successors and assigns, from and against any and all costs, expenses, attorney's fees, losses, damages and liabilities incurred or suffered directly or indirectly from or attributable to any claims arising out of the negligent acts, errors or omissions, or willful misconduct of the Consultant, or its officers, agents, employees, subconsultants, licensees or invitees of the Consultant, except to the extent caused by the negligent acts, errors or omissions, or willful misconduct of the County. The Consultant expressly understands and agrees that any Performance Bond or insurance protection required of the Consultant, or otherwise provided by the Consultant, shall in no way limit the responsibility to indemnify the County as hereinabove provided.

h) Confidentiality and Ownership of Documents

Consultant acknowledges and agrees that information regarding this Contract is confidential and shall not be disclosed, directly, indirectly or by implication, or be used by Consultant in any way, whether during the term of this Contract or at any time thereafter, except solely as required in the course of Consultant's performance hereunder. Consultant shall comply with the applicable privacy laws and regulations affecting County and will not disclose any of County's records, materials, or other data to any third party. Consultant shall not have the right to compile and distribute statistical analyses and reports utilizing data derived from information or data obtained from County without the prior written approval of County. In the event such approval is given, any such reports published and distributed by Consultant shall be furnished to County without charge.

All documents, data, studies, reports, work product or product created as a result of the performance of the Contract (the "Documents") shall be included in the Deliverables and shall be the property of the County of Cook. It shall be a breach of this Contract for the Consultant to reproduce or use any documents, data, studies, reports, work product or product obtained from the County of Cook or any Documents created hereby, whether such reproduction or use is for Consultant's own purposes or for those of any third party. During the performance of the Contract Consultant shall be responsible of any loss or damage to the Documents while they are in Consultant's possession, and any such loss or damage shall be restored at the expense of the Consultant. The County and its designees shall be afforded full access to the Documents and the work at all times.

i) Patents, Copyrights and Licenses

If applicable, Consultant shall furnish the Chief Procurement Officer with all licenses

required for the County to utilize any software, including firmware or middleware, provided by Consultant as part of the Deliverables. Such licenses shall be clearly marked with a reference to the number of this County Contract. Consultant shall also furnish a copy of such licenses to the Chief Procurement Officer.

Consultant agrees to hold harmless and indemnify the County, its officers, agents, employees and affiliates from and defend, as permitted by Illinois law, at its own expense (including reasonable attorneys', accountants' and consultants' fees), any suit or proceeding brought against County based upon a claim that the ownership and/or use of equipment, hardware and software or any part thereof provided to the County or utilized in performing Consultant's services constitutes an infringement of any patent, copyright or license or any other property right.

In the event the use of any equipment, hardware or software or any part thereof is enjoined, Consultant with all reasonable speed and due diligence shall provide or otherwise secure for County, at the Consultant's election, one of the following: the right to continue use of the equipment, hardware or software; an equivalent system having the Specifications as provided in this Contract; or Consultant shall modify the system or its component parts so that they become non-infringing while performing in a substantially similar manner to the original system, meeting the requirements of this Contract.

j) Examination of Records and Audits

The Consultant agrees that the Cook County Auditor or any of its duly authorized representatives shall, until expiration of three (3) years after the final payment under the Contract, have access and the right to examine any books, documents, papers, canceled checks, bank statements, purveyor's and other invoices, and records of the Consultant related to the Contract, or to Consultant's compliance with any term, condition or provision thereof. The Consultant shall be responsible for establishing and maintaining records sufficient to document the costs associated with performance under the terms of this Contract.

The Consultant further agrees that it shall include in all of its subcontracts hereunder a provision to the effect that the Subcontractor agrees that the Cook County Auditor or any of its duly authorized representatives shall, until expiration of three (3) years after final payment under the subcontract, have access and the right to examine any books, documents, papers, canceled checks, bank statements, purveyor's and other invoices and records of such Subcontractor involving transactions relating to the subcontract, or to such Subcontractor compliance with any term, condition or provision thereunder or under the Contract.

In the event the Consultant receives payment under the Contract, reimbursement for which is later disallowed by the County, the Consultant shall promptly refund the disallowed amount to the County on request, or at the County's option, the County may credit the amount disallowed from the next payment due or to become due to the Consultant under any contract with the County.

To the extent this Contract pertains to Deliverables which may be reimbursable under the Medicaid or Medicare Programs, Consultant shall retain and make available upon request, for a period of four (4) years after furnishing services pursuant to this Agreement, the contract, books, documents and records which are necessary to certify the nature and extent of the costs of such services if requested by the Secretary of Health and Human Services or the Comptroller General of the United States or any of their duly authorized representatives.

If Consultant carries out any of its duties under the Agreement through a subcontract with a related organization involving a value of cost of $10,000.00 or more over a 12 month period, Consultant will cause such subcontract to contain a clause to the effect that, until the expiration of four years after the furnishing of any service pursuant to said subcontract, the related organization will make available upon request of the Secretary of Health and Human Services or the Comptroller General of the United States or any of their duly authorized representatives, copies of said subcontract and any books, documents, records and other data of said related organization that are necessary to certify the nature and extent of such costs. This paragraph relating to the retention and production of documents is included because of possible application of Section 1861(v)(1)(I) of the Social Security Act to this Agreement; if this Section should be found to be inapplicable, then this paragraph shall be deemed inoperative and without force and effect.

k) Subcontracting or Assignment of Contract or Contract Funds

Once awarded, this Contract shall not be subcontracted or assigned, in whole or in part, without the advance written approval of the Chief Procurement Officer, which approval shall be granted or withheld at the sole discretion of the Chief Procurement Officer. In no case, however, shall such approval relieve the Consultant from its obligations or change the terms of the Contract. The Consultant shall not transfer or assign any Contract funds or any interest therein due or to become due without the advance written approval of the Chief Procurement Officer. The unauthorized subcontracting or assignment of the Contract, in whole or in part, or the unauthorized transfer or assignment of any Contract funds, either in whole or in part, or any interest therein, which shall be due or are to become due the Consultant shall have no effect on the County and are null and void. Notwithstanding the foregoing, Consultant may assign this Agreement, its rights, or obligations without consent: (a) to an affiliate or subsidiary; or (b) for purposes of financing, merger, acquisition, corporate reorganization, or sale of all or substantially all its assets.

Prior to the commencement of the Contract, the Consultant shall identify in writing to the Chief Procurement Officer the names of any and all Subcontractors it intends to use in the performance of the Contract by completing the Identification of Subcontractor/Supplier/ Subconsultant Form ("ISF"). The Chief Procurement Officer shall have the right to disapprove any Subcontractor. All Subcontractors shall be subject to the terms of this Contract. Consultant shall incorporate into all subcontracts all of the provisions of the Contract which affect such subcontract. Copies of subcontracts shall be provided to the Chief Procurement Officer upon request.

The Consultant must disclose the name and business address of each Subcontractor, attorney, lobbyist, accountant, consultant and any other person or entity whom the Consultant has retained or expects to retain in connection with the Matter, as well as the nature of the relationship, and the total amount of the fees paid or estimated to be paid. The Consultant is not required to disclose employees who are paid or estimated to be paid. The Consultant is not required to disclose employees who are paid solely through the Consultant's regular payroll. "Lobbyist" means any person or entity who undertakes to influence any legislation or administrative action on behalf of any person or entity other than: (1) a not-for-profit entity, on an unpaid basis, or (2), himself.

"Lobbyist" also means any person or entity any part of whose duties as an employee of another includes undertaking to influence any legislative or administrative action. If the Consultant is uncertain whether a disclosure is required under this Section, the Consultant must either ask the County, whether disclosure is required or make the disclosure.

The County reserves the right to prohibit any person from entering any County facility for any reason. All Consultants and Subcontractor of the Consultant shall be accountable to the Chief Procurement Officer or his designee while on any County property and shall abide by all rules and regulations imposed by the County.

l) Intentionally Omitted

ARTICLE 4) TERM OF PERFORMANCE

a) Term of Performance

This Agreement takes effect when approved by the Cook County Board and its term shall begin on **January 1, 2026** ("**Effective Date**") and continue until **December 31, 2030** or until this Agreement is terminated in accordance with its terms, whichever occurs first.

b) Timeliness of Performance

i) Consultant must provide the Services and Deliverables within the term and within the time limits required under this Agreement, pursuant to the provisions of Section 4.a and Exhibit 1. Further, Consultant acknowledges that TIME IS OF THE ESSENCE and that the failure of Consultant to comply with the time limits described in this Section 4.b may result in economic or other losses to the County.

ii) Neither Consultant nor Consultant's agents, employees nor Subcontractors are entitled to any damages from the County, nor is any party entitled to be reimbursed by the County, for damages, charges or other losses or expenses incurred by Consultant by reason of delays or hindrances in the performance of the Services, whether or not caused by the County.

c) Agreement Extension Option

The Chief Procurement Officer may at any time before this Agreement expires elect to renew this Agreement for **two (2) two-year renewal options, and one (1) one-year renewal option** under the same terms and conditions as this original Agreement, except as provided otherwise in this Agreement, by notice in writing to Consultant. After notification by the Chief Procurement Officer, this Agreement must be modified to reflect the time extension in accordance with the provisions of Section 10.c.

ARTICLE 5) COMPENSATION

a) Basis of Payment

The County will pay Consultant according to the Schedule of Compensation in the attached Exhibit 1 for the successful completion of services.

b) Method of Payment

All invoices submitted by the Consultant shall be in accordance with the cost provisions contained in the Agreement and shall contain a detailed description of the Deliverables, including the quantity of the Deliverables, for which payment is requested. All invoices for services shall include itemized entries indicating the date or time period in which the services were provided, the amount of time spent performing the services, and a detailed description of the services provided during the period of the invoice. All Contracts for services that are procured as Sole Source must also contain a provision requiring the Contractor to submit itemized records indicating the dates that services were provided, a detailed description of the work performed on each such date, and the amount of time spent performing work on each such date. All invoices shall reflect the amounts invoiced by and the amounts paid to the Consultant as of the date of the invoice. Invoices for new charges shall not include "past due" amounts, if any, which amounts must be set forth on a separate invoice. Consultant shall not be entitled to invoice the County for any late fees or other penalties.

In accordance with Section 34-177 of the Cook County Procurement Code, the County shall have a right to set off and subtract from any invoice(s) or Contract price, a sum equal to any fines and penalties, including interest, for any tax or fee delinquency and any debt or obligation owed by the Consultant to the County.

The Consultant acknowledges its duty to ensure the accuracy of all invoices submitted to the County for payment. By submitting the invoices, the Consultant certifies that all itemized entries set forth in the invoices are true and correct. The Consultant acknowledges that by submitting the invoices, it certifies that it has delivered the Deliverables, i.e., the goods, supplies, services or equipment set forth in the Agreement to the Using Agency, or that it has properly performed the services set forth in the Agreement. The invoice must also reflect the dates and amount of time expended in the provision of services under the Agreement. The Consultant acknowledges that any inaccurate statements or negligent or intentional

misrepresentations in the invoices shall result in the County exercising all remedies available to it in law and equity including, but not limited to, a delay in payment or non-payment to the Consultant, and reporting the matter to the Cook County Office of the Independent Inspector General.

When a Consultant receives any payment from the County for any supplies, equipment, goods, or services, it has provided to the County pursuant to its Agreement, the Consultant must make payment to its Subcontractors within 15 days after receipt of payment from the County, provided that such Subcontractor has satisfactorily provided the supplies, equipment, goods or services in accordance with the Contract and provided the Consultant with all of the documents and information required of the Consultant. The Consultant may delay or postpone payment to a Subcontractor when the Subcontractor's supplies, equipment, goods, or services do not comply with the requirements of the Contract, the Consultant is acting in good faith, and not in retaliation for a Subcontractor exercising legal or contractual rights.

c) Funding

The source of funds for payments under this Agreement is identified in Exhibit 1, Schedule of Compensation. Payments under this Agreement must not exceed the dollar amount shown in Exhibit 1 without a written amendment in accordance with Section 10.c.

d) Non-Appropriation

If no funds or insufficient funds are appropriated and budgeted in any fiscal period of the County for payments to be made under this Agreement, then the County will notify Consultant in writing of that occurrence, and this Agreement will terminate on the earlier of the last day of the fiscal period for which sufficient appropriation was made or whenever the funds appropriated for payment under this Agreement are exhausted. Payments for Services completed to the date of notification will be made to Consultant. No payments will be made or due to Consultant and under this Agreement beyond those amounts appropriated and budgeted by the County to fund payments under this Agreement.

e) Taxes

Federal Excise Tax does not apply to materials purchased by the County by virtue of Exemption Certificate No. 36-75-0038K. Illinois Retailers' Occupation Tax, Use Tax and Municipal Retailers' Occupation Tax do not apply to deliverables, materials or services purchased by the County by virtue of statute. The price or prices quoted herein shall include any and all other federal and/or state, direct and/or indirect taxes which apply to this Contract. The County's State of Illinois Sales Tax Exemption Identification No. is E-9998-2013-07.

f) Price Reduction

If at any time after the contract award, Consultant makes a general price reduction in the price of any of the Deliverables, the equivalent price reduction based on similar quantities and/or considerations shall apply to this Contract for the duration of the Contract period. For

purposes of this Section 5.f., Price Reduction, a general price reduction shall include reductions in the effective price charged by Consultant by reason of rebates, financial incentives, discounts, value points or other benefits with respect to the purchase of the Deliverables. Such price reductions shall be effective at the same time and in the same manner as the reduction Consultant makes in the price of the Deliverables to its prospective customers generally.

g) Consultant Credits

To the extent the Consultant gives credits toward future purchases of goods or services, financial incentives, discounts, value points or other benefits based on the purchase of the materials or services provided for under this Contract, such credits belong to the County and not any specific Using Agency. Consultant shall reflect any such credits on its invoices and in the amounts it invoices the County.

ARTICLE 6) DISPUTES

Any dispute arising under the Contract between the County and Consultant shall be decided by the Chief Procurement Officer. The complaining party shall submit a written statement detailing the dispute and specifying the specific relevant Contract provision(s) to the Chief Procurement Officer. Upon request of the Chief Procurement Officer, the party complained against shall respond to the complaint in writing within five days of such request. The Chief Procurement Officer will reduce her decision to writing and mail or otherwise furnish a copy thereof to the Consultant. The decision of the Chief Procurement Officer will be final and binding. Dispute resolution as provided herein shall be a condition precedent to any other action at law or in equity. However, unless a notice is issued by the Chief Procurement Officer indicating that additional time is required to review a dispute, the parties may exercise their contractual remedies, if any, if no decision is made within sixty (60) days following notification to the Chief Procurement Officer of a dispute. No inference shall be drawn from the absence of a decision by the Chief Procurement Officer.
Notwithstanding a dispute, Consultant shall continue to discharge all its obligations, duties and responsibilities set forth in the Contract during any dispute resolution proceeding unless otherwise agreed to by the County in writing.

ARTICLE 7) COOPERATION WITH INSPECTOR GENERAL AND COMPLIANCE WITH ALL LAWS

The Consultant, Subcontractor, licensees, grantees or persons or businesses who have a County contract, grant, license, or certification of eligibility for County contracts shall abide by all of the applicable provisions of the Office of the Independent Inspector General Ordinance (Section 2-281 et. seq. of the Cook County Code of Ordinances). Failure to cooperate as required may result in monetary and/or other penalties.

The Consultant shall observe and comply with the laws, ordinances, regulations and codes of the Federal, State, County and other local government agencies which may in any manner affect the

performance of the Contract including, but not limited to, those County Ordinances set forth in the Certifications attached hereto and incorporated herein. Assurance of compliance with this requirement by the Consultant's employees, agents or Subcontractor shall be the responsibility of the Consultant.

The Consultant shall secure and pay for all federal, state and local licenses, permits and fees required hereunder.

ARTICLE 8) SPECIAL CONDITIONS

a) Warranties and Representations

In connection with signing and carrying out this Agreement, Consultant:

i) warrants that Consultant is appropriately licensed under Illinois law to perform the Services required under this Agreement and will perform no Services for which a professional license is required by law and for which Consultant is not appropriately licensed;

ii) warrants it is financially solvent; it and each of its employees, agents and Subcontractors of any tier are competent to perform the Services required under this Agreement; and Consultant is legally authorized to execute and perform or cause to be performed this Agreement under the terms and conditions stated in this Agreement;

iii) warrants that it will not knowingly use the services of any ineligible consultant or Subcontractor for any purpose in the performance of its Services under this Agreement;

iv) warrants that Consultant and its Subcontractors are not in default at the time this Agreement is signed, and has not been considered by the Chief Procurement Officer to have, within 5 years immediately preceding the date of this Agreement, been found to be in default on any contract awarded by the County;

v) represents that it has carefully examined and analyzed the provisions and requirements of this Agreement; it understands the nature of the Services required; from its own analysis it has satisfied itself as to the nature of all things needed for the performance of this Agreement; this Agreement is feasible of performance in accordance with all of its provisions and requirements, and Consultant warrants it can and will perform, or cause to be performed, the Services in strict accordance with the provisions and requirements of this Agreement;

vi) represents that Consultant and, to the best of its knowledge, its Subcontractors are not in violation of the provisions of the Illinois Criminal Code, 720 ILCS 5/33E as amended; and

vii) acknowledges that any certification, affidavit or acknowledgment made under oath in connection with this Agreement is made under penalty of perjury and, if false, is also cause for termination under Sections 9.a and 9.c.

b) Ethics

i) In addition to the foregoing warranties and representations, Consultant warrants:

(1) no officer, agent or employee of the County is employed by Consultant or has a financial interest directly or indirectly in this Agreement or the compensation to be paid under this Agreement except as may be permitted in writing by the Board of Ethics.

(2) no payment, gratuity or offer of employment will be made in connection with this Agreement by or on behalf of any Subcontractors to the prime Consultant or higher tier Subcontractors or anyone associated with them, as an inducement for the award of a subcontract or order.

c) Joint and Several Liability

If Consultant, or its successors or assigns, if any, is comprised of more than one individual or other legal entity (or a combination of them), then under this Agreement, each and without limitation every obligation or undertaking in this Agreement to be fulfilled or performed by Consultant is the joint and several obligation or undertaking of each such individual or other legal entity.

d) Business Documents

At the request of the County, Consultant must provide copies of its latest articles of incorporation, by-laws and resolutions, or partnership or joint venture agreement, as applicable.

e) Conflicts of Interest

i) No member of the governing body of the County or other unit of government and no other officer, employee or agent of the County or other unit of government who exercises any functions or responsibilities in connection with the Services to which this Agreement pertains is permitted to have any personal interest, direct or indirect, in this Agreement. No member of or delegate to the Congress of the United States or the Illinois General Assembly and no Commissioner of the Cook County Board or County employee is allowed to be admitted to any share or part of this Agreement or to any financial benefit to arise from it.

ii) Consultant covenants that it, and to the best of its knowledge, its Subcontractors if any (collectively, "**Consulting Parties**"), presently have no direct or indirect interest and will not acquire any interest, direct or indirect, in any project or contract

that would conflict in any manner or degree with the performance of its Services under this Agreement.

iii) Upon the request of the County, Consultant must disclose to the County its past client list and the names of any clients with whom it has an ongoing relationship. Consultant is not permitted to perform any Services for the County on applications or other documents submitted to the County by any of Consultant's past or present clients. If Consultant becomes aware of a conflict, it must immediately stop work on the assignment causing the conflict and notify the County.

iv) Without limiting the foregoing, if the Consulting Parties assist the County in determining the advisability or feasibility of a project or in recommending, researching, preparing, drafting or issuing a request for proposals or bid specifications for a project, the Consulting Parties must not participate, directly or indirectly, as a prime, Subcontractor or joint venturer in that project or in the preparation of a proposal or bid for that project during the term of this Agreement or afterwards. The Consulting Parties may, however, assist the County in reviewing the proposals or bids for the project if none of the Consulting Parties have a relationship with the persons or entities that submitted the proposals or bids for that project.

v) The Consultant further covenants that, in the performance of this Agreement, no person having any conflicting interest will be assigned to perform any Services or have access to any confidential information, as defined in Section 3.h of this Agreement. If the County, by the Chief Procurement Officer in his reasonable judgment, determines that any of Consultant's Services for others conflict with the Services Consultant is to render for the County under this Agreement, Consultant must terminate such other services immediately upon request of the County.

vi) Furthermore, if any federal funds are to be used to compensate or reimburse Consultant under this Agreement, Consultant represents that it is and will remain in compliance with federal restrictions on lobbying set forth in Section 319 of the Department of the Interior and Related Agencies Appropriations Act for Fiscal year 1990, 31 U.S.C. § 1352, and related rules and regulations set forth at 54 Fed. Reg. 52,309 ff. (1989), as amended. If federal funds are to be used, Consultant must execute a Certification Regarding Lobbying, which will be attached as an exhibit and incorporated by reference as if fully set forth here.

f) Non-Liability of Public Officials

Consultant and any assignee or Subcontractor of Consultant must not charge any official, employee or agent of the County personally with any liability or expenses of defense or hold any official, employee or agent of the County personally liable to them under any term or provision of this Agreement or because of the County's execution, attempted execution or any breach of this Agreement.

ARTICLE 9) EVENTS OF DEFAULT, REMEDIES, TERMINATION, SUSPENSION AND RIGHT TO OFFSET

a) Events of Default Defined

The following constitute events of default:

i) Any material misrepresentation, whether negligent or willful and whether in the inducement or in the performance, made by Consultant to the County.

ii) Consultant's material failure to perform any of its obligations under this Agreement including the following:

(a) Failure due to a reason or circumstances within Consultant's reasonable control to perform the Services with sufficient personnel and equipment or with sufficient material to ensure the performance of the Services;

(b) Failure to perform the Services in a manner reasonably satisfactory to the Chief Procurement Officer or inability to perform the Services satisfactorily as a result of insolvency, filing for bankruptcy or assignment for the benefit of creditors;

(c) Failure to promptly re-perform within a reasonable time Services that were rejected as erroneous or unsatisfactory;

(d) Discontinuance of the Services for reasons within Consultant's reasonable control; and

(e) Failure to comply with any other material term of this Agreement, including the provisions concerning insurance and nondiscrimination.

iii) Any change in ownership or control of Consultant without the prior written approval of the Chief Procurement Officer, which approval the Chief Procurement Officer will not unreasonably withhold.

iv) Consultant's default under any other agreement it may presently have or may enter into with the County during the life of this Agreement. Consultant acknowledges and agrees that in the event of a default under this Agreement the County may also declare a default under any such other Agreements.

v) Failure to comply with Article 7 in the performance of the Agreement.

vi) Consultant’s repeated or continued violations of County ordinances unrelated to performance under the Agreement that in the opinion of the Chief Procurement Officer indicate a willful or reckless disregard for County laws and regulations.

b) Remedies

The occurrence of any event of default permits the County, at the County's sole option, to declare Consultant in default. The Chief Procurement Officer may in his sole discretion give Consultant an opportunity to cure the default within a certain period of time, which period of time must not exceed 30 days, unless extended by the Chief Procurement Officer. Whether to declare Consultant in default is within the sole discretion of the Chief Procurement Officer and neither that decision nor the factual basis for it is subject to review or challenge under the Disputes provision of this Agreement.

The Chief Procurement Officer will give Consultant written notice of the default, either in the form of a cure notice ("**Cure Notice**"), or, if no opportunity to cure will be granted, a default notice ("**Default Notice**"). If the Chief Procurement Officer gives a Default Notice, he will also indicate any present intent he may have to terminate this Agreement, and the decision to terminate (but not the decision not to terminate) is final and effective upon giving the notice. The Chief Procurement Officer may give a Default Notice if Consultant fails to affect a cure within the cure period given in a Cure Notice. When a Default Notice with intent to terminate is given as provided in this Section 9.b and Article 11, Consultant must discontinue any Services, unless otherwise directed in the notice, and deliver all materials accumulated in the performance of this Agreement, whether completed or in the process, to the County. After giving a Default Notice, the County may invoke any or all of the following remedies:

i) The right to take over and complete the Services, or any part of them, at Consultant's expense and as agent for Consultant, either directly or through others, and bill Consultant for the cost of the Services, and Consultant must pay the difference between the total amount of this bill and the amount the County would have paid Consultant under the terms and conditions of this Agreement for the Services that were assumed by the County as agent for the Consultant under this Section 9.b;

ii) The right to terminate this Agreement as to any or all of the Services yet to be performed effective at a time specified by the County;

iii) The right of specific performance, an injunction or any other appropriate equitable remedy;

iv) The right to money damages;

v) The right to withhold all or any part of Consultant's compensation under this Agreement;

vi) The right to consider Consultant non-responsible in future contracts to be awarded by the County.

If the Chief Procurement Officer considers it to be in the County's best interests, he may elect not to declare default or to terminate this Agreement. The parties acknowledge that this provision is solely for the benefit of the County and that if the County permits Consultant to continue to provide the Services despite one or more events of default, Consultant is in no way relieved of any of its responsibilities, duties or obligations under this Agreement, nor does the County waive or relinquish any of its rights.

The remedies under the terms of this Agreement are not intended to be exclusive of any other remedies provided, but each and every such remedy is cumulative and is in addition to any other remedies, existing now or later, at law, in equity or by statute. No delay or omission to exercise any right or power accruing upon any event of default impairs any such right or power, nor is it a waiver of any event of default nor acquiescence in it, and every such right and power may be exercised from time to time and as often as the County considers expedient.

c) Early Termination

In addition to termination under Sections 9.a and 9.b of this Agreement, the County may terminate this Agreement, or all or any portion of the Services to be performed under it, at any time by a notice in writing from the County to Consultant. The County will give notice to Consultant in accordance with the provisions of Article 11. The effective date of termination will be thirty (30) days from the date the notice is received by Consultant or the date stated in the notice, whichever is later. If the County elects to terminate this Agreement in full, all Services to be provided under it must cease and all materials that may have been accumulated in performing this Agreement, whether completed or in the process, must be delivered to the County within thirty (30) days after the date the notice is considered received as provided under Article 11 of this Agreement (if no date is given) or upon the effective date stated in the notice.

After the notice is received, Consultant must restrict its activities, and those of its Subcontractors, to winding down any reports, analyses, or other activities previously begun. No costs incurred after the effective date of the termination are allowed. Payment for any Services actually and satisfactorily performed before the effective date of the termination is on the same basis as set forth in Article 5, but if any compensation is described or provided for on the basis of a period longer than 10 days, then the compensation must be prorated accordingly. No amount of compensation, however, is permitted for anticipated profits on unperformed Services. The County and Consultant must attempt to agree on the amount of compensation to be paid to Consultant, but if not agreed on, the dispute must be settled in accordance with Article 6 of this Agreement. The payment so made to Consultant is in full settlement for all Services satisfactorily performed under this Agreement.

Consultant must include in its contracts with Subcontractors an early termination provision in form and substance equivalent to this early termination provision to prevent claims against the County arising from termination of subcontracts after the early termination. Consultant will not be entitled to make any early termination claims against the County

resulting from any Subcontractor's claims against Consultant or the County to the extent inconsistent with this provision.

If the County's election to terminate this Agreement for default under Sections 9.a and 9.b is determined in a court of competent jurisdiction to have been wrongful, then in that case the termination is to be considered to be an early termination under this Section 9.c.

d) Suspension

The County may at any time request that Consultant suspend its Services, or any part of them, by giving 15 days prior written notice to Consultant or upon informal oral, or even no notice, in the event of emergency. No costs incurred after the effective date of such suspension are allowed. Consultant must promptly resume its performance of the Services under the same terms and conditions as stated in this Agreement upon written notice by the Chief Procurement Officer and such equitable extension of time as may be mutually agreed upon by the Chief Procurement Officer and Consultant when necessary for continuation or completion of Services. Any additional costs or expenses actually incurred by Consultant as a result of recommencing the Services must be treated in accordance with the compensation provisions under Article 5 of this Agreement.

No suspension of this Agreement is permitted in the aggregate to exceed a period of 45 days within any one year of this Agreement. If the total number of days of suspension exceeds 45 days, Consultant by written notice may treat the suspension as an early termination of this Agreement under Section 9.c.

e) Right to Offset

In connection with performance under this Agreement, the County may offset any excess costs incurred:

i) if the County terminates this Agreement for default or any other reason resulting from Consultant's performance or non-performance;

ii) if the County exercises any of its remedies under Section 9.b of this Agreement; or

iii) if the County has any credits due or has made any overpayments under this Agreement.

The County may offset these excess costs by use of any payment due for Services completed before the County terminated this Agreement or before the County exercised any remedies. If the amount offset is insufficient to cover those excess costs, Consultant is liable for and must promptly remit to the County the balance upon written demand for it. This right to offset is in addition to and not a limitation of any other remedies available to the County.

f) Delays

Consultant agrees that no charges or claims for damages shall be made by Consultant for any delays or hindrances from any cause whatsoever during the progress of any portion of this Contract.

g) Prepaid Fees

In the event this Contract is terminated by either party, for cause or otherwise, and the County has prepaid for any Deliverables, Consultant shall refund to the County, on a prorated basis to the effective date of termination, all amounts prepaid for Deliverables not actually provided as of the effective date of the termination. The refund shall be made within fourteen (14) days of the effective date of termination.

ARTICLE 10) GENERAL CONDITIONS

a) Entire Agreement

i) **General**

This Agreement, and the exhibits attached to it and incorporated in it, constitute the entire agreement between the parties and no other warranties, inducements, considerations, promises or interpretations are implied or impressed upon this Agreement that are not expressly addressed in this Agreement.

ii) **No Collateral Agreements**

Consultant acknowledges that, except only for those representations, statements or promises expressly contained in this Agreement and any exhibits attached to it and incorporated by reference in it, no representation, statement or promise, oral or in writing, of any kind whatsoever, by the County, its officials, agents or employees, has induced Consultant to enter into this Agreement or has been relied upon by Consultant, including any with reference to:

(a) the meaning, correctness, suitability or completeness of any provisions or requirements of this Agreement;

(b) the nature of the Services to be performed;
(c) the nature, quantity, quality or volume of any materials, equipment, labor and other facilities needed for the performance of this Agreement;

(d) the general conditions which may in any way affect this Agreement or its performance;

(e) the compensation provisions of this Agreement; or

(f) any other matters, whether similar to or different from those referred to in (a) through (e) immediately above, affecting or having any connection with this Agreement, its negotiation, any discussions of its performance or those employed or connected or concerned with it.

iii) **No Omissions**

Consultant acknowledges that Consultant was given an opportunity to review all documents forming this Agreement before signing this Agreement in order that it might request inclusion in this Agreement of any statement, representation, promise or provision that it desired or on that it wished to place reliance. Consultant did so review those documents, and either every such statement, representation, promise or provision has been included in this Agreement or else, if omitted, Consultant relinquishes the benefit of any such omitted statement, representation, promise or provision and is willing to perform this Agreement in its entirety without claiming reliance on it or making any other claim on account of its omission.

b) Counterparts

This Agreement is comprised of several identical counterparts, each to be fully signed by the parties and each to be considered an original having identical legal effect.

c) Contract Amendments

The parties may during the term of the Contract make amendments to the Contract but only as provided in this section. Such amendments shall only be made by mutual agreement in writing.

In the case of Contracts not approved by the Board, the Chief Procurement Officer may amend a contract provided that the total cost of all such amendments does not increase the total amount of the Contract by $200,000 or more. Such action may only be made with the advance written approval of the Chief Procurement Officer. If the amendment increases the total award amount by $200,000 or more, then Board approval will be required.

No Using Agency or employee thereof has authority to make any amendments to this Contract. Any amendments to this Contract made without the express written approval of the Chief Procurement Officer is void and unenforceable.

Consultant is hereby notified that, except for amendments which are made in accordance with this Section10. c. Contract Amendments, no Using Agency or employee thereof has authority to make any amendment to this Contract.

d) Governing Law and Jurisdiction

This Contract shall be governed by and construed under the laws of the State of Illinois. The Consultant irrevocably agrees that, subject to the County's sole and absolute election to the contrary, any action or proceeding in any way, manner or respect arising out of the Contract,

or arising from any dispute or controversy arising in connection with or related to the Contract, shall be litigated only in courts within the Circuit Court of Cook County, State of Illinois, and the Consultant consents and submits to the jurisdiction thereof. In accordance with these provisions, Consultant waives any right it may have to transfer or change the venue of any litigation brought against it by the County pursuant to this Contract.

e) Severability

If any provision of this Agreement is held or considered to be or is in fact invalid, illegal, inoperative or unenforceable as applied in any particular case in any jurisdiction or in all cases because it conflicts with any other provision or provisions of this Agreement or of any constitution, statute, ordinance, rule of law or public policy, or for any other reason, those circumstances do not have the effect of rendering the provision in question invalid, illegal, inoperative or unenforceable in any other case or circumstances, or of rendering any other provision or provisions in this Agreement invalid, illegal, inoperative or unenforceable to any extent whatsoever. The invalidity, illegality, inoperativeness or unenforceability of any one or more phrases, sentences, clauses or sections in this Agreement does not affect the remaining portions of this Agreement or any part of it.

f) Assigns

All of the terms and conditions of this Agreement are binding upon and inure to the benefit of the parties and their respective legal representatives, successors and assigns.

g) Cooperation

Consultant must at all times cooperate fully with the County and act in the County's best interests. If this Agreement is terminated for any reason, or if it is to expire on its own terms, Consultant must make every effort to assure an orderly transition to another provider of the Services, if any, orderly demobilization of its own operations in connection with the Services, uninterrupted provision of Services during any transition period and must otherwise comply with the reasonable requests and requirements of the Using Agency in connection with the termination or expiration.

h) Waiver

Nothing in this Agreement authorizes the waiver of a requirement or condition contrary to law or ordinance or that would result in or promote the violation of any federal, state or local law or ordinance.

Whenever under this Agreement the County by a proper authority waives Consultant's performance in any respect or waives a requirement or condition to either the County's or Consultant's performance, the waiver so granted, whether express or implied, only applies to the particular instance and is not a waiver forever or for subsequent instances of the performance, requirement or condition. No such waiver is a modification of this Agreement regardless of the number of times the County may have waived the

performance, requirement or condition. Such waivers must be provided to Consultant in writing.

i) Independent Consultant

This Agreement is not intended to and will not constitute, create, give rise to, or otherwise recognize a joint venture, partnership, corporation or other formal business association or organization of any kind between Consultant and the County. The rights and the obligations of the parties are only those expressly set forth in this Agreement. Consultant must perform under this Agreement as an independent Consultant and not as a representative, employee, agent, or partner of the County.

This Agreement is between the County and an independent Consultant and, if Consultant is an individual, nothing provided for under this Agreement constitutes or implies an employer-employee relationship such that:

i) The County will not be liable under or by reason of this Agreement for the payment of any compensation award or damages in connection with the Consultant performing the Services required under this Agreement.

ii) Consultant is not entitled to membership in the County Pension Fund, Group Medical Insurance Program, Group Dental Program, Group Vision Care, Group Life Insurance Program, Deferred Income Program, vacation, sick leave, extended sick leave, or any other benefits ordinarily provided to individuals employed and paid through the regular payrolls of the County.

iv) The County is not required to deduct or withhold any taxes, FICA or other deductions from any compensation provided to the Consultant.

j) Governmental Joint Purchasing Agreement

Pursuant to Section 4 of the Illinois Governmental Joint Purchasing Act (30 ILCS 525) and the Joint Purchase Agreement approved by the Cook County Board of Commissioners (April 9, 1965), other units of government may purchase goods or services under this contract.

In the event that other agencies participate in a joint procurement, the County reserves the right to renegotiate the price to accommodate the larger volume.

k) Comparable Government Procurement

As permitted by the County of Cook, other government entities, if authorized by law, may wish to purchase the goods, supplies, services or equipment under the same terms and conditions contained in this Contract (i.e., comparable government procurement). Each entity wishing to reference this Contract must have prior authorization from the County of Cook and the Consultant. If such participation is authorized, all purchase orders will be

issued directly from and shipped directly to the entity requiring the goods, supplies, equipment or services supplies/services. The County shall not be held responsible for any orders placed, deliveries made or payment for the goods, supplies, equipment or services supplies/services ordered by these entities. Each entity reserves the right to determine the amount of goods, supplies, equipment or services it wishes to purchase under this Contract.

l) Force Majeure

Neither Consultant nor County shall be liable for failing to fulfill any obligation under this Contract if such failure is caused by an event beyond such party's reasonable control and which is not caused by such party's fault or negligence. Such events shall be limited to acts of God, acts of war, fires, lightning, floods, epidemics, or riots.

m) Intentionally Omitted

ARTICLE 11) NOTICES

All notices required pursuant to this Contract shall be in writing and addressed to the parties at their respective addresses set forth below. All such notices shall be deemed duly given if hand delivered or if deposited in the United States mail, postage prepaid, registered or certified, return receipt requested. Notice as provided herein does not waive service of summons or process.

If to the County: Cook County States Attorney Office
69 W. Washington Street, Suite 3200
Chicago, Illinois 60602
Attention: Darren Ganir, Chief Information Officer

and

Cook County Chief Procurement Officer
161 N. Clark Street, Suite 2300
Chicago, Illinois 60601
(Include County Contract Number on all notices)

If to Consultant: Axon Enterprise, Inc.
18700 N. 85th St.
Scottsdale, AZ 85255
legal@axon.com
Attention: Legal Department

Changes in these addresses must be in writing and delivered in accordance with the provisions of this Article 11. Notices delivered by mail are considered received three days after mailing in accordance with Article 11. Notices delivered personally are considered effective upon receipt. Refusal to accept delivery has the same effect as receipt.

ARTICLE 12) AUTHORITY

Execution of this Agreement by Consultant is authorized by a resolution of its Board of Directors, if a corporation, or similar governing document, and the signature(s) of each person signing on behalf of Consultant have been made with complete and full authority to commit Consultant to all terms and conditions of this Agreement, including each and every representation, certification and warranty contained in it, including the representations, certifications and warranties collectively incorporated by reference in it.

EXHIBIT 1

Axon Quote Summary

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

Q-690161-45936AR

Issued: 10/06/2025

Quote Expiration: 11/30/2025

Estimated Contract Start Date: 01/01/2026

Account Number: 483844

Payment Terms: N30

Mode of Delivery: UPS-GND

Credit/Debit Amount: $0.00

SHIP TO	BILL TO
69 W. Washington, Suite 3200 69 W Washington St Ste 3200 Chicago, IL 60602-3174 USA	Cook County (IL) State's Attorney Office 69 W Washington St Ste 3200 Chicago IL 60602-3174 USA Email:

SALES REPRESENTATIVE	PRIMARY CONTACT
Dave Swanson Phone: Email: dswanson@axon.com Fax:	Darren Ganir Phone: 312-603-1877 Email: darren.ganir@cookcountysao.org Fax:

Quote Summary

Program Length	60 Months
TOTAL COST	$11,101,643.12
ESTIMATED TOTAL W/ TAX	$11,101,643.12

Renewal Program Length #1	24 Months
TOTAL COST	$5,101,258.39
ESTIMATED TOTAL W/ TAX	$5,101,258.39

Renewal Program Length #3	12 Months
TOTAL COST	$2,924,741.41
ESTIMATED TOTAL W/ TAX	$2,924,741.41

Discount Summary

Average Savings Per Year	$2,536,422.20
TOTAL SAVINGS	$25,364,222.00

Renewal Program Length #2	24 Months
TOTAL COST	$5,517,521.08
ESTIMATED TOTAL W/ TAX	$5,517,521.08

Payment Summary

Date	Subtotal	Tax	Total
Dec 2025	$1,839,665.93	$0.00	$1,839,665.93
Jan 2026	$185,000.00	$0.00	$185,000.00
Dec 2026	$2,137,537.77	$0.00	$2,137,537.77
Dec 2027	$2,223,039.28	$0.00	$2,223,039.28
Dec 2028	$2,311,960.85	$0.00	$2,311,960.85
Dec 2029	$2,404,439.29	$0.00	$2,404,439.29
Dec 2030	$2,500,616.86	$0.00	$2,500,616.86
Dec 2031	$2,600,641.53	$0.00	$2,600,641.53
Dec 2032	$2,704,667.20	$0.00	$2,704,667.20
Dec 2033	$2,812,853.88	$0.00	$2,812,853.88
Dec 2034	$2,924,741.41	$0.00	$2,924,741.41
Total	**$24,645,164.00**	**$0.00**	**$24,645,164.00**

Quote Unbundled Price:	**$50,012,224.00**
Quote List Price:	**$31,902,172.00**
Quote Subtotal:	**$24,645,164.00**

Pricing

All deliverables are detailed in Delivery Schedules section lower in proposal

Item	Description	Qty	Term	Unbundled	List Price	Net Price	Subtotal	Tax	Total
Program									
S00019	BUNDLE - JUSTICE PREMIER PLUS	1290	120	$295.88	$178.89	$144.93	$22,435,164.00	$0.00	$22,435,164.00
A la Carte Services									
101616	AXON EVIDENCE - CHANNEL SERVICES - ADDITIONAL 100 TB	40			$50,000.00	$0.00	$0.00	$0.00	$0.00
101345	AXON JUSTICE - PSO - PREMIUM DEPLOYMENT	1			$30,000.00	$30,000.00	$30,000.00	$0.00	$30,000.00
101192	AXON JUSTICE - LEGACY MIGRATION	1			$50,000.00	$50,000.00	$50,000.00	$0.00	$50,000.00
101161	AXON - REGIONAL SWS TECHNICAL ACCOUNT MANAGER	1	12		$6,250.00	$6,250.00	$75,000.00	$0.00	$75,000.00
100578	AXON JUSTICE - PSO - IMPLEMENTATION	525			$200.00	$200.00	$105,000.00	$0.00	$105,000.00
101616	AXON EVIDENCE - CHANNEL SERVICES - ADDITIONAL 100 TB	39			$50,000.00	$50,000.00	$1,950,000.00	$0.00	$1,950,000.00
Total							**$24,645,164.00**	**$0.00**	**$24,645,164.00**

Delivery Schedule

Software

Bundle	Item	Description	QTY	Estimated Start Date	Estimated End Date
BUNDLE - JUSTICE PREMIER PLUS	100165	AXON EVIDENCE - STORAGE - THIRD PARTY UNLIMITED	1290	01/01/2026	12/31/2035
BUNDLE - JUSTICE PREMIER PLUS	100789	AXON INVESTIGATE - UPGRADE TO PRO ACCESS	1290	01/01/2026	12/31/2035
BUNDLE - JUSTICE PREMIER PLUS	101866	AXON BRIEF ONE FOR JUSTICE	1290	01/01/2026	12/31/2035
BUNDLE - JUSTICE PREMIER PLUS	101905	POLICY CHAT	1290	01/01/2026	12/31/2035
BUNDLE - JUSTICE PREMIER PLUS	73478	AXON EVIDENCE - REDACTION ASSISTANT USER LICENSE	1290	01/01/2026	12/31/2035
BUNDLE - JUSTICE PREMIER PLUS	73618	AXON COMMUNITY REQUEST	1290	01/01/2026	12/31/2035
BUNDLE - JUSTICE PREMIER PLUS	73686	AXON EVIDENCE - STORAGE - UNLIMITED (AXON DEVICE)	1290	01/01/2026	12/31/2035
BUNDLE - JUSTICE PREMIER PLUS	73838	AXON EVIDENCE - ECOM LICENSE - PRO FOR PROSECUTOR	1290	01/01/2026	12/31/2035
BUNDLE - JUSTICE PREMIER PLUS	85762	AXON AUTO-TRANSCRIBE - JUSTICE ACCESS	1290	01/01/2026	12/31/2035
BUNDLE - JUSTICE PREMIER PLUS	85767	AXON EVIDENCE - DISCOVERY MODULE ACCESS	1290	01/01/2026	12/31/2035

Services

Bundle	Item	Description	QTY
BUNDLE - JUSTICE PREMIER PLUS	101184	AXON INVESTIGATE - TRAINING - OPERATOR AND EXAMINER	86
BUNDLE - JUSTICE PREMIER PLUS	11642	AXON INVESTIGATE - THIRD PARTY VIDEO SUPPORT	1290
A la Carte	100578	AXON JUSTICE - PSO - IMPLEMENTATION	525
A la Carte	101161	AXON - REGIONAL SWS TECHNICAL ACCOUNT MANAGER	1
A la Carte	101192	AXON JUSTICE - LEGACY MIGRATION	1

Services

Bundle	Item	Description	QTY
A la Carte	101345	AXON JUSTICE - PSO - PREMIUM DEPLOYMENT	1
A la Carte	101616	AXON EVIDENCE - CHANNEL SERVICES - ADDITIONAL 100 TB	39
A la Carte	101616	AXON EVIDENCE - CHANNEL SERVICES - ADDITIONAL 100 TB	40

Shipping Locations

Location Number	Street	City	State	Zip	Country
1	69 W Washington St Ste 3200	Chicago	IL	60602-3174	USA

Payment Details

Dec 2025

Invoice Plan	Item	Description	Qty	Subtotal	Tax	Total
Annual Payment 1	101161	AXON - REGIONAL SWS TECHNICAL ACCOUNT MANAGER	1	$5,640.80	$0.00	$5,640.80
Annual Payment 1	101616	AXON EVIDENCE - CHANNEL SERVICES - ADDITIONAL 100 TB	39	$146,660.85	$0.00	$146,660.85
Annual Payment 1	S00019	BUNDLE - JUSTICE PREMIER PLUS	1290	$1,687,364.28	$0.00	$1,687,364.28
Total				**$1,839,665.93**	**$0.00**	**$1,839,665.93**

Jan 2026

Invoice Plan	Item	Description	Qty	Subtotal	Tax	Total
Invoice Upon Fulfillment	100578	AXON JUSTICE - PSO - IMPLEMENTATION	525	$105,000.00	$0.00	$105,000.00
Invoice Upon Fulfillment	101192	AXON JUSTICE - LEGACY MIGRATION	1	$50,000.00	$0.00	$50,000.00
Invoice Upon Fulfillment	101345	AXON JUSTICE - PSO - PREMIUM DEPLOYMENT	1	$30,000.00	$0.00	$30,000.00
Invoice Upon Fulfillment	101616	AXON EVIDENCE - CHANNEL SERVICES - ADDITIONAL 100 TB	40	$0.00	$0.00	$0.00
Total				**$185,000.00**	**$0.00**	**$185,000.00**

Dec 2026

Invoice Plan	Item	Description	Qty	Subtotal	Tax	Total
Annual Payment 2	101161	AXON - REGIONAL SWS TECHNICAL ACCOUNT MANAGER	1	$6,554.14	$0.00	$6,554.14
Annual Payment 2	101616	AXON EVIDENCE - CHANNEL SERVICES - ADDITIONAL 100 TB	39	$170,407.63	$0.00	$170,407.63
Annual Payment 2	S00019	BUNDLE - JUSTICE PREMIER PLUS	1290	$1,960,576.00	$0.00	$1,960,576.00
Total				**$2,137,537.77**	**$0.00**	**$2,137,537.77**

Dec 2027

Invoice Plan	Item	Description	Qty	Subtotal	Tax	Total
Annual Payment 3	101161	AXON - REGIONAL SWS TECHNICAL ACCOUNT MANAGER	1	$6,816.31	$0.00	$6,816.31
Annual Payment 3	101616	AXON EVIDENCE - CHANNEL SERVICES - ADDITIONAL 100 TB	39	$177,223.94	$0.00	$177,223.94
Annual Payment 3	S00019	BUNDLE - JUSTICE PREMIER PLUS	1290	$2,038,999.03	$0.00	$2,038,999.03
Total				**$2,223,039.28**	**$0.00**	**$2,223,039.28**

Dec 2028

Invoice Plan	Item	Description	Qty	Subtotal	Tax	Total
Annual Payment 4	101161	AXON - REGIONAL SWS TECHNICAL ACCOUNT MANAGER	1	$7,088.96	$0.00	$7,088.96
Annual Payment 4	101616	AXON EVIDENCE - CHANNEL SERVICES - ADDITIONAL 100 TB	39	$184,312.90	$0.00	$184,312.90
Annual Payment 4	S00019	BUNDLE - JUSTICE PREMIER PLUS	1290	$2,120,558.99	$0.00	$2,120,558.99
Total				**$2,311,960.85**	**$0.00**	**$2,311,960.85**

Dec 2029

Invoice Plan	Item	Description	Qty	Subtotal	Tax	Total
Annual Payment 5	101161	AXON - REGIONAL SWS TECHNICAL ACCOUNT MANAGER	1	$7,372.52	$0.00	$7,372.52

Dec 2029

Invoice Plan	Item	Description	Qty	Subtotal	Tax	Total
Annual Payment 5	101616	AXON EVIDENCE - CHANNEL SERVICES - ADDITIONAL 100 TB	39	$191,685.41	$0.00	$191,685.41
Annual Payment 5	S00019	BUNDLE - JUSTICE PREMIER PLUS	1290	$2,205,381.36	$0.00	$2,205,381.36
Total				**$2,404,439.29**	**$0.00**	**$2,404,439.29**

Dec 2030

Invoice Plan	Item	Description	Qty	Subtotal	Tax	Total
Annual Payment 6	101161	AXON - REGIONAL SWS TECHNICAL ACCOUNT MANAGER	1	$7,667.42	$0.00	$7,667.42
Annual Payment 6	101616	AXON EVIDENCE - CHANNEL SERVICES - ADDITIONAL 100 TB	39	$199,352.83	$0.00	$199,352.83
Annual Payment 6	S00019	BUNDLE - JUSTICE PREMIER PLUS	1290	$2,293,596.61	$0.00	$2,293,596.61
Total				**$2,500,616.86**	**$0.00**	**$2,500,616.86**

Dec 2031

Invoice Plan	Item	Description	Qty	Subtotal	Tax	Total
Annual Payment 7	101161	AXON - REGIONAL SWS TECHNICAL ACCOUNT MANAGER	1	$7,974.11	$0.00	$7,974.11
Annual Payment 7	101616	AXON EVIDENCE - CHANNEL SERVICES - ADDITIONAL 100 TB	39	$207,326.94	$0.00	$207,326.94
Annual Payment 7	S00019	BUNDLE - JUSTICE PREMIER PLUS	1290	$2,385,340.48	$0.00	$2,385,340.48
Total				**$2,600,641.53**	**$0.00**	**$2,600,641.53**

Dec 2032

Invoice Plan	Item	Description	Qty	Subtotal	Tax	Total
Annual Payment 8	101161	AXON - REGIONAL SWS TECHNICAL ACCOUNT MANAGER	1	$8,293.08	$0.00	$8,293.08
Annual Payment 8	101616	AXON EVIDENCE - CHANNEL SERVICES - ADDITIONAL 100 TB	39	$215,620.02	$0.00	$215,620.02
Annual Payment 8	S00019	BUNDLE - JUSTICE PREMIER PLUS	1290	$2,480,754.10	$0.00	$2,480,754.10
Total				**$2,704,667.20**	**$0.00**	**$2,704,667.20**

Dec 2033

Invoice Plan	Item	Description	Qty	Subtotal	Tax	Total
Annual Payment 9	101161	AXON - REGIONAL SWS TECHNICAL ACCOUNT MANAGER	1	$8,624.80	$0.00	$8,624.80
Annual Payment 9	101616	AXON EVIDENCE - CHANNEL SERVICES - ADDITIONAL 100 TB	39	$224,244.82	$0.00	$224,244.82
Annual Payment 9	S00019	BUNDLE - JUSTICE PREMIER PLUS	1290	$2,579,984.26	$0.00	$2,579,984.26
Total				**$2,812,853.88**	**$0.00**	**$2,812,853.88**

Dec 2034

Invoice Plan	Item	Description	Qty	Subtotal	Tax	Total
Annual Payment 10	101161	AXON - REGIONAL SWS TECHNICAL ACCOUNT MANAGER	1	$8,967.87	$0.00	$8,967.87
Annual Payment 10	101616	AXON EVIDENCE - CHANNEL SERVICES - ADDITIONAL 100 TB	39	$233,164.66	$0.00	$233,164.66
Annual Payment 10	S00019	BUNDLE - JUSTICE PREMIER PLUS	1290	$2,682,608.88	$0.00	$2,682,608.88
Total				**$2,924,741.41**	**$0.00**	**$2,924,741.41**

EXHIBIT 2

Axon Online Support Platforms Terms of Use

Axon Online Support Platforms Terms of Use Appendix

1 **Definitions**.

"**Axon Online Support Platforms**" means Axon Academy and MyAxon.

"**Axon Academy**" means Axon's Customer learning management system on absorblms.com, and other related offerings, including, without limitation, interactions between Axon Academy and Axon Products.

"**MyAxon**" means Axon's Customer support portal hosted on salesforce.com and other related offerings, including, without limitation, interactions between MyAxon and Axon Products.

"**Axon Online Customer Content**" means

a) "Academy Customer Content" is data uploaded into, ingested by, or created in Axon Academy within Customer's tenant, including training materials, media or multimedia uploaded into Axon Academy by Customer. Academy Customer Content excludes Academy Non-Content Data.

b) "MyAxon Customer Content" means data uploaded into, ingested by, or created in MyAxon within Customer's tenant, including, without limitation, media or multimedia uploaded into MyAxon by Customer. MyAxon Customer Content excludes MyAxon Non-Content Data.

"**Axon Online Non-Content Data**" means

a) "Academy Non-Content Data" is data, configuration, and usage information about Customer's Axon Academy tenant, Axon Devices and client software, and users that is transmitted or generated when using Axon Academy. Academy Non-Content Data includes data about users captured during account management and customer support activities. Academy Non-Content Data does not include Academy Customer Content.

b) "MyAxon Non-Content Data" is data, configuration, and usage information about Customer's MyAxon tenant, Axon Devices and client software, and users that is transmitted or generated when using MyAxon. MyAxon Non-Content Data includes data about users captured during account management and customer support activities. MyAxon Non-Content Data does not include MyAxon Customer Content.

"**Axon Support Materials**" means material(s) or content(s) made available by Axon to Customer within MyAxon or Axon Academy.

"**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.

2 **Access**. Upon Axon granting Customer a subscription to Axon Online Support Platforms, Customer may access and use Axon Online Support Platforms to store and manage Axon Online Customer Content.

3 **Customer Owns Axon Online Customer Content**. Customer controls and owns all right, title,

and interest in Axon Online Customer Content. Except as outlined herein, Axon obtains no interest in Axon Online Customer Content, and Axon Online Customer Content is not Axon's business records. Except as set forth in this Agreement, Agency is responsible for uploading, sharing, managing, and deleting Axon Online Customer Content. Axon will only have access to Axon Online Customer Content for the limited purposes set forth herein. Customer agrees to allow Axon access to Axon Online Customer Content to (a) perform troubleshooting, maintenance, or diagnostic screenings; and (b) enforce this Agreement or policies governing use of Axon Online Support Platforms and other Axon Products.

4 **Security**. Axon will implement commercially reasonable and appropriate measures to secure Axon Online Customer Content against accidental or unlawful loss, access, or disclosure. Axon will maintain a comprehensive information security program to protect Axon Online Customer Content including logical, physical access, vulnerability, risk, and configuration management; incident monitoring and response; security education; and data protection.

5 **Customer Responsibilities**. Customer is responsible for (a) ensuring Customer owns Axon Online Customer Content; (b) ensuring no Axon Online Customer Content or Customer end user's use of Axon Online Customer Content or Axon Online Support Platforms violates this Agreement or applicable laws; and (c) maintaining necessary computer equipment and Internet connections for use of Axon Online Support Platforms. 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 Online Support Platforms.

Customer will also maintain the security of end usernames and passwords and security and access by end users to Axon Online Customer Content. Customer is responsible for ensuring the configuration and utilization of Axon Online Support Platforms meets applicable Customer policies, regulations, and standards. Customer may not sell, transfer, or sublicense access to any other entity or person. Customer shall contact Axon immediately if an unauthorized party may be using Customer's account or Axon Online Customer Content, or if account information is lost or stolen.

6 **Privacy**. Customer's use of Axon Online Support Platforms is subject to the Axon Online Support Platforms Privacy Policy, a current version of which is available at https://www.axon.com/legal/axon-online-support-platforms-privacy-policy. Customer agrees to allow Axon access to Axon Online Non-Content Data from Customer to (a) perform troubleshooting, maintenance, or diagnostic screenings; (b) provide, develop, improve, and support current and future Axon Products including Axon Online Support Platforms and related services; and (c) enforce this Agreement or policies governing the use of Axon Products. Data controlled by Absorb Software Inc. is subject to the Absorb LMS Privacy Policy. Data controlled by Salesforce.com, Inc. is subject to the Salesforce.com Privacy Policy.

7 **Location of Storage**. Axon may transfer Axon Online Customer Content and Axon Online Non-Content Data to third-party subcontractors for Processing. Axon will determine the locations for Processing of Axon Online Customer Content and Axon Online Non-Content Data. For all customers, Axon will Process including store Axon Online Customer Content and Axon Online Non-Content Data within the United States. Ownership of Axon Online Customer Content remains with Customer. Customer acknowledges that Processing, including storage, of Axon Online Customer Content and Axon Online Non-Content Data will be in the United States.

8 **Suspension**. Axon may temporarily suspend Customer's or any end user's right to access or use any portion or all of Axon Online Support Platforms immediately upon notice, if Customer or end user's use of or registration for Axon Online Support Platforms may (a) pose a security risk to Axon Products including Axon Online Support Platforms, or any third-party; (b) adversely impact Axon Online Support Platforms, 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 Axon Online Customer Content because of suspension, except as specified in this Agreement.

9 **Axon Online Support Platforms Warranty**. Axon disclaims any warranties or responsibility for data corruption or errors which occur on Axon Online Support Platforms.

10 **Axon Online Support Platforms Restrictions**. Customer and Customer end users (including employees, contractors, agents, officers, volunteers, and directors), may not, or may not attempt to:

10.1 copy, modify, tamper with, repair, or create derivative works of any part of Axon Online Support Platforms;

10.2 reverse engineer, disassemble, or decompile Axon Online Support Platforms or apply any process to derive any source code included in Axon Online Support Platforms, or allow others to do the same;

10.3 access or use Axon Online Support Platforms with the intent to gain unauthorized access, avoid incurring fees or exceeding usage limits or quotas;

10.4 use trade secret information contained in Axon Online Support Platforms, except as expressly permitted in this Agreement;

10.5 access Axon Online Support Platforms to build a competitive product or service or copy any features, functions, or graphics of Axon Online Support Platforms;

10.6 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 Online Support Platforms; or

10.7 use Axon Online Support Platforms to store or transmit infringing, libelous, or other unlawful or tortious material; to store or transmit material in violation of third-party privacy rights; or to store or transmit malicious code.

EXHIBIT 3

Axon Master Services and Purchasing Agreement

Exhibit 3 - Master Services and Purchasing Agreement for Customer

This Master Services and Purchasing Agreement ("**MSPA**") is between Axon Enterprise, Inc. ("**Axon**"), and Cook County ("**Customer**"). Axon and Customer are each a "**Party**" and collectively "**Parties**". This Agreement governs Customer's purchase and use of the Axon Devices and Services detailed in the Quote Appendix ("**Quote**"). . The Parties agree as follows:

1. **Definitions**.

   1.1. "**Axon Cloud Services**" means Axon's web services, including but not limited to, Axon Evidence, Axon Records, Axon Dispatch, FUSUS services and interactions between Axon Evidence and Axon Devices or Axon client software. Axon Cloud Service excludes third-party applications, hardware warranties, and my.evidence.com.

   1.2. "**Axon Device**" means all hardware provided by Axon under this MSPA. 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 MSPA, including software, Axon Cloud Services, and professional services.

2. **Term**. The Term of this MSPA is as set forth in Article 4 of the Professional Services Agreement ("**Term**").

   2.1. All subscriptions including Axon Evidence, Axon Fleet, Officer Safety Plans, Technology Assurance Plans, and TASER 7 or TASER 10 plans begin on the date stated in the Quote. Each subscription term ends upon completion of the subscription stated in the Quote ("**Subscription Term**").

   2.2. Intentionally Omitted.

3. **Intentionally Omitted**.

4. **Intentionally Omitted**.

5. **Shipping**. Axon may make partial shipments and ship Axon Devices from multiple locations. All Agreement goods, equipment or supplies shipped to the County shall be shipped F.O.B., DESTINATION, FREIGHT PREPAID. Arrangements shall be made in advance by Axon in order that the County may arrange for receipt of the materials. Customer is responsible for any shipping charges in the Quote.

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

7. **Warranty**.

   7.1. **Limited Warranty**. Axon warrants that Axon-manufactured Devices are free from defects in workmanship and materials for one (1) year from the date of Customer's receipt, except Signal Sidearm and Axon-manufactured accessories, which Axon warrants for thirty (30) months and ninety (90) days, respectively, from the date of Customer's receipt. Used conducted energy weapon ("**CEW**") cartridges are deemed to have operated properly. Extended warranties run from the expiration of the one (1) year hardware warranty through the extended warranty term purchased.

   7.2. **Disclaimer. Except as set forth in the Agreement, 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.**

   7.3. **Claims**. If Axon receives a valid warranty claim for an Axon-manufactured Device during the warranty term, Axon's shall, within thirty (30) days, 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.

      7.3.1. 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.

7.4. **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 under Section 5. Axon assumes no liability or obligation in the event Customer does not utilize Spare Axon Devices for the intended purpose.

7.5. **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 serial number that was materially defaced or removed after delivery to Customer. Axon's warranty will be void if Customer resells Axon Devices.

7.5.1. To the extent permitted by law, and except as otherwise set forth in the Agreement, the above warranties are exclusive. Axon disclaims all other warranties, 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, it 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.

7.5.2. Neither Party will be liable for special, indirect, incidental, punitive or consequential damages, however caused, whether for breach of warranty or contract, negligence, strict liability, tort or any other legal theory

7.6. **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.

7.7. .

7.8. **Intentionally Omitted**.

8. **Intentionally Omitted**.

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

10. **Design Changes**. Axon may make design 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. **Bundled Offerings**. Some offerings in bundled offerings may not be generally available at the time of Customer's purchase. Axon may, at its sole discretion, provide a refund, credit, or additional discount beyond what is in the Quote due to Customer's election not to utilize any portion of an Axon bundle.

12. **Intentionally Omitted**.

13. **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 intentionally cause any Axon proprietary rights to be violated.

14. **IP Indemnification**. Axon will indemnify Customer against all claims, losses, and reasonable expenses from any third-party claim alleging that the use of Axon-manufactured Devices or Services infringes or misappropriates the third-party's intellectual property rights. Customer must promptly provide Axon with written notice of such claim, tender to Axon the defense or settlement of such claim at Axon's expense and reasonably cooperate with Axon in the defense or settlement of such claim. Axon's IP indemnification obligations do not apply to claims based on (a) modification of Axon-manufactured Devices or Services by Customer or a third-party not approved or recommended by Axon; (b) use of Axon-manufactured Devices and Services in combination with hardware or services not approved or recommended by Axon; (c) use of Axon Devices and Services other than as permitted in this Agreement; or (d) use of Axon software that is not the most current release provided by Axon provided that (a) Customer is responsible for installing such updates pursuant to the terms of the Agreement (b) the updates do not materially degrade the functionality of the software, (c) the update is offered at no additional cost or expense to Customer, and (d) Customer has received prior notice that such update/s are available and has been afforded reasonable time to install the update/s.

15. **Customer Responsibilities**. Customer is responsible for (a) Customer's use of Axon Devices; (b) breach of this Agreement or violation of applicable law by Customer or an Customer end user; (c) disputes between Customer and a third-party over Customer's use of Axon Devices to the extent not arising from Axon's gross negligence, willful misconduct, or infringement of intellectual property (c) ensuring Axon Devices are destroyed and disposed of securely and sustainably at Customer's cost;and (e) any regulatory violations or fines, as a result of Customer's improper destruction or disposal of Axon Devices.

16. **Termination**.

    16.1. **Intentionally Omitted**.

    16.2 **Intentionally Omitted**

    16.3 **Intentionally Omitted**

17. **Confidentiality**. "**Confidential Information**" means nonpublic information designated as confidential or, given the nature of the information or circumstances surrounding disclosure, should reasonably be understood to be confidential. If Customer receives a public records request to disclose information that Axon has designated as Confidential, to the extent allowed by law, Customer sole obligation will provide notice to Axon before disclosure.

18. **General**.

    18.1. **Intentionally Omitted**.

    18.2. **Intentionally Omitted**.

    18.3. **Third-Party Beneficiaries**. There are no third-party beneficiaries under this Agreement.

    18.4. **Non-Discrimination**. Neither Party nor its employees will discriminate against any person based on race; religion; creed; color; sex; gender identity and expression; pregnancy; childbirth; breastfeeding; medical conditions related to pregnancy, childbirth, or breastfeeding; sexual orientation; marital status; age; national origin; ancestry; genetic information; disability; veteran status; or any class protected by local, state, or federal law.

    18.5. **Export Compliance**. Each Party will comply with all import and export control laws and regulations.

    18.6. .

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

    18.8. **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.

    18.9. **Survival**. The following sections will survive termination: Payment, Warranty, Axon Device Warnings, Indemnification, IP Rights, Customer Responsibilities and any other Sections detailed in the survival sections of the Appendices.

    18.10. **Intentionally Omitted**.

    18.11. **Intentionally Omitted**.

    18.12 **Intentionally Omitted**.

Axon Cloud Services Terms of Use Appendix

1. Definitions.

   a. **"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.

   b. "**Evidence**" is media or multimedia uploaded into Axon Evidence as 'evidence' by an Customer. Evidence is a subset of Customer Content.

   c. "**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.

   d. "**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.

   e. "**Provided Data**" means de-identified, de-personalized, data, which cannot be re-identified or re-personalized, derived from Customer's TASER energy weapon deployment reports, related TASER energy weapon logs, body-worn camera footage, and incident reports.

   f. "**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 more end users than the Quote specifies. Axon Air requires an Axon Evidence subscription for each drone operator. For Axon Evidence Lite, Customer may access and use Axon Evidence only to store and manage TASER CEW and TASER CAM data ("**TASER Data**"). Customer may not upload non-TASER Data to Axon Evidence Lite.

3. **Customer Owns Customer Content**. Customer controls and owns all right, 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 management systems or records.

5. **Customer Responsibilities**. Customer is responsible for (a) ensuring Customer owns 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; and (c) maintaining necessary computer equipment and Internet connections for use of Axon Cloud Services. 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.

   Customer will also maintain the security of end 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. 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.

6. **Privacy**. Customer's use of Axon Cloud Services is subject to the Axon Cloud Services Privacy Policy, attached to this Cloud Services Terms of Use Appendix. 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. **Axon Body Wi-Fi Positioning**. Axon Body cameras may offer a feature to enhance location services where GPS/GNSS signals may not be available, for instance, within buildings or underground. Customer administrators can manage their choice to use this service within the administrative features of Axon Cloud Services. If Customer chooses to use this service, Axon must also enable the usage of the feature for Customer's Axon Cloud Services tenant. Customer will not see this option with Axon Cloud Services unless Axon has enabled Wi-Fi Positioning for Customer's Axon Cloud Services tenant. When Wi-Fi Positioning is enabled by both Axon and Customer, Non-Content and Personal Data will be sent to Skyhook Holdings, Inc. ("**Skyhook**") to facilitate the Wi-Fi Positioning functionality. Data controlled by Skyhook is outside the scope of the Axon Cloud Services Privacy Policy and is subject to the Skyhook Services Privacy Policy.

8. **Storage**. For Axon Unlimited Device Storage subscriptions, Customer may store unlimited data in Customer's Axon Evidence account only if data originates from Axon Capture or the applicable 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.

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

9. **Location of Storage**. Axon may transfer Customer Content to third-party subcontractors for storage who are bound by written contracts with Axon that impose data protection terms that are not less protective than those imposed by the Professional Services Agreement, including Exhibit 3 (ITSCs) and Exhibit 4 (CJIS). Axon will at all times be responsible for maintaining the confidentiality of Customer Content, even when transferred to a third-party subcontractor. Axon will determine the locations of data centers for storage of Customer Content. For United States agencies, Axon will ensure all Agency Content stored in Axon Cloud Services remains within the United States. Ownership of Customer Content remains with Customer.

10. **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 it reasonably determines that 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) materially 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.. Axon will not delete Customer Content because of suspension, except as specified in this Agreement.

11. **Axon Cloud Services Warranty**. Axon disclaims any warranties or responsibility for data corruption or errors before Customer uploads data to Axon Cloud Services.

12. **TASER Data Science Program**. Axon will provide a quantitative evaluation on the performance and effectiveness of TASER energy weapons in the field across a variety of circumstances.

13. If Customer purchases the TASER Data Science Program, Customer grants Axon, its affiliates, and assignees an irrevocable, perpetual, fully paid, royalty-free, and worldwide right and license to use Provided Data solely for the purposes of this Agreement and to create Transformed Data. Customer shall own all rights and title to Provided Data. Axon shall own all rights and title to Transformed Data and any derivatives of Transformed Data.

14. Axon grants to Customer an irrevocable, perpetual, fully paid, royalty-free, license to use to TASER Data Science report provided to Customer for its own internal purposes. **The Data Science report is provided "as is" and without any warranty of any kind.**

15. In the event Customer seeks Axon's deletion of Provided Data, it may submit a request to privacy@axon.com. Where reasonably capable of doing so, Axon will promptly implement the request but at a minimum will not continue to collect Provided Data from Customer.

16. **Axon Records**. Axon Records is the software-as-a-service product that is generally available at the time Customer purchases an OSP 7 or OSP 10 bundle. During Customer's Axon Records Subscription Term, if any, Customer will be entitled to receive Axon's Update and Upgrade releases on an if-and-when available basis.

    The Axon Records Subscription Term will end upon the completion of the Axon Records Subscription as documented in the Quote, or if purchased as part of an OSP 7 or OSP 10 bundle, upon completion of the OSP 7 or OSP 10 Term ("**Axon Records Subscription**")

    An "**Update**" is a generally available release of Axon Records that Axon makes available from time to time. An "**Upgrade**" includes (i) new versions of Axon Records that enhance features and functionality, as solely determined by Axon; and/or (ii) new versions of Axon Records that provide additional features or perform additional functions. Upgrades exclude new products that Axon introduces and markets as distinct products or applications.

    New or additional Axon products and applications, as well as any Axon professional services needed to configure Axon Records, are not included. If Customer purchases Axon Records as part of a bundled offering, the Axon Record subscription begins on the later of the (1) start date of that bundled offering, or (2) date Axon provisions Axon Records to Customer.

    Users of Axon Records at the Customer may upload files to entities (incidents, reports, cases, etc) in Axon Records with no limit to the number of files and amount of storage. Notwithstanding the foregoing, Axon may limit usage should the Customer exceed an average rate of one-hundred (100) GB per user per year of uploaded files. Axon will not bill for overages.

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

    a) 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;

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

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

    d) use Axon Cloud Serves as a service bureau, or as part of an Customer infrastructure as a service;

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

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

    g) 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

    h) 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.

18. **Axon Narrative.** AI-Assisted Report Writing feature. Axon may impose usage restrictions if a single user generates more than one hundred (100) reports per month for two or more consecutive months.

19. **After Termination**. Axon will not delete Customer Content for one hundred and eighty (180) days following termination. There will be no functionality of Axon Cloud Services during these one hundred and eighty (180) 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 one hundred and eighty (180) 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.

20. **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.

21. **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.

22. **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 Cloud Services Privacy Policy

Last Updated: August 9th, 2021

*This Axon Cloud Services Privacy Policy ("**Policy**") applies only to the information that Axon Enterprise, Inc. ("**Axon**") collects and you or your employer (collectively, "**Customer**") 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 Privacy Policy. Usage of Axon Citizen is governed by the Axon Citizen Privacy Policy.*

Unless otherwise provided in this Policy, this Policy is subject to the terms of the Master Services Purchasing Agreement, or other similar agreement, if any, between Axon and Customer ("**Agreement**"). To the extent this Policy contains terms and conditions that differ from those contained in the Agreement, the Agreement shall control. A concept or principle covered in this Policy 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 and defined terms referenced, but not defined, in this Policy shall have the meanings assigned to them in the Agreement.

Axon complies with the EU-U.S. Privacy Shield Framework and the Swiss-U.S. Privacy Shield Framework ("Privacy Shield") as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal information transferred from the European Union, the United Kingdom, and Switzerland to the United States in reliance on Privacy Shield. Axon has certified to the U.S. Department of Commerce that it adheres to the Privacy Shield Principles with respect to such information. If any conflict exists between the terms of this Policy and the Privacy Shield Principles, the Privacy Shield Principles shall govern. To learn more about the Privacy Shield program, and to view our certification, please visit https://www.privacyshield.gov/.

By using Axon Cloud Services, Customer acknowledges that Customer has read and understand this Policy and Customer agrees to be bound by its terms and conditions. Axon may occasionally update this Policy. 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 agreement and acceptance to any such changes.

Definitions

- "**Axon Cloud Services**" means Axon's web services hosted on evidence.com including **Axon Evidence**, **Axon Records,** and **Axon Dispatch**, 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 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 and users;
  (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.

  For purposes of clarity, Customer Content does not include Non-Content Data, and Non-Content Data does not include Customer Content.
- **"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.
- **"Data Exporter"** means the Data Controller who transfers the Personal Data.
- **"Data Importer"** means the Data Processor who agrees to receive from the Data Exporter Personal Data intended for processing on Data Exporter's behalf after the transfer in accordance with the Agreement and who is not subject to a third country's system ensuring adequate protection with in the meaning of the General Data Protection Regulation (EU) 2016/679 of the European Parliament ("**GDPR**")
- **"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.

- "**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 processor engaged by the Data Importer or by any other sub-processor of the Data Importer who agrees to receive from the Data Importer or from any other sub-processor of the Data Importer Personal Data exclusively intended for processing activities to be carried out on behalf of the Data Exporter after the transfer in accordance with its instructions, the terms of the Clauses and the terms of the written subcontract.

Axon's Role

Axon is a Data Processor of Customer Content. Customer controls and owns all right, title, and interest in and to Customer Content and Axon obtains no rights to the Customer Content. Customer is solely responsible for the uploading, sharing, withdrawal, management and deletion of Customer Content. Customer grants Axon limited access to Customer Content solely to provide and support Axon Cloud Services to and for Customer and Customer's end-users. Customer represents and warrants to Axon that: (1) Customer owns Customer Content; (2) and Customer Content, and Customer's end-users' use of Customer Content and Axon Cloud Services, does not violate this Policy or applicable data protection laws and regulations.

Axon may also collect, control, and process Non-Content Data. Axon is a Data Controller for Non-Content Data. Axon collects, controls, and processes Non-Content Data to provide Axon Cloud Services and to support the overall delivery of Axon Products including business, operational, and security purposes. With Non-Content Data, Axon may analyze and report anonymized and aggregated data to communicate with external and internal stakeholders. In regard to Customer Entity & User Data, Axon is a Data Controller and Customer is an independent Data Controller, not a joint Data Controller with Customer.

Data Collection and Processing Activities

CUSTOMER CONTENT

Axon will only use Customer Content to provide Customer Axon Cloud Services. Axon will not use Customer Content for any advertising or similar 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. Changes to Axon Cloud Services may increase the capabilities of the service and ways in which Customer Content can be processed.

NON-CONTENT DATA

Non-Content Data includes data, configuration, and usage information about customer's Axon Cloud Services tenant, Axon Devices, Axon Client Applications, and users that is transmitted or generated when using Axon Products. Non-Content Data includes the following:

Customer Entity And User Data

Customer Entity and User Data includes personal and non-personal data regarding Customer's Axon Cloud Services tenant configuration and users. 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 but may unsubscribe from promotional communications at any time.

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 uses 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 uses Service Operations and Security Data to provide service operations and monitoring.

Account Data

Axon uses Account Data to provide Axon Cloud Services, manage Customer's accounts, market to, and communicate with Customer. Customer may unsubscribe from promotional communications at any time.

Support Data

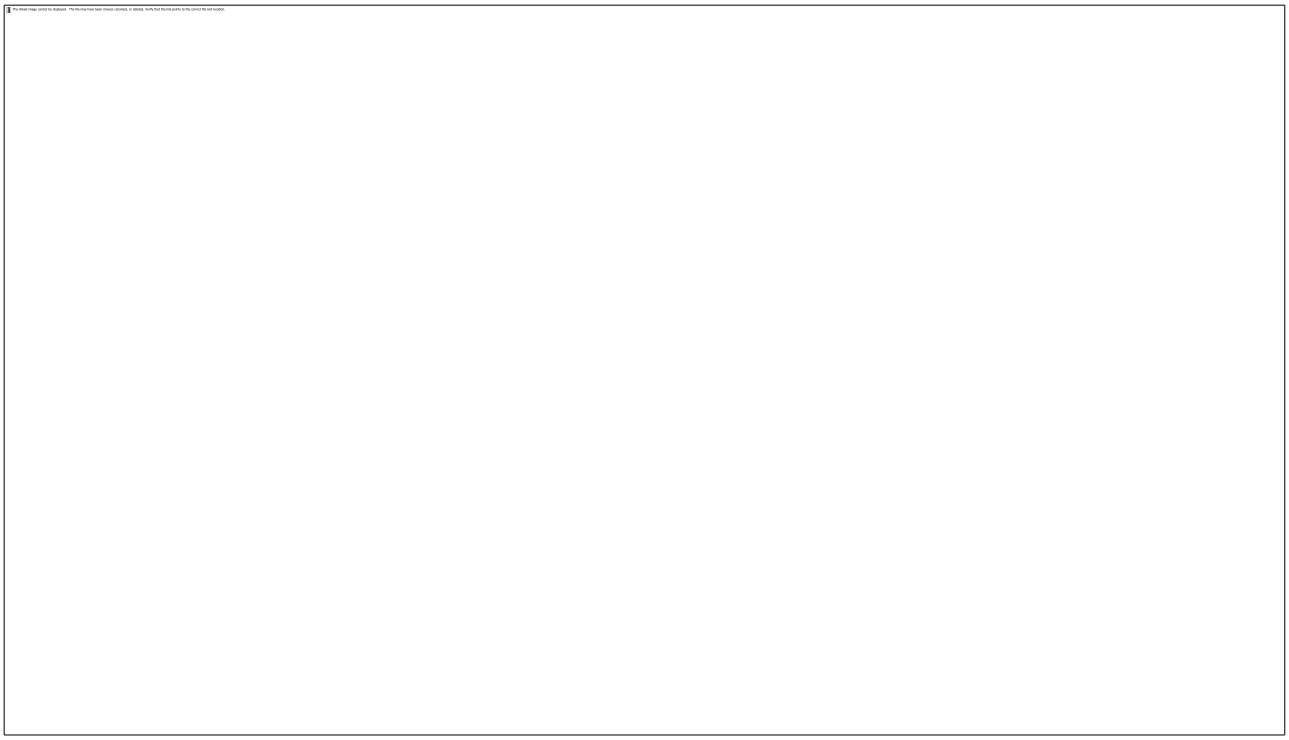
Axon uses Support Data to resolve Customer’s support incident, and to operate, improve, and personalize Axon Products. If Customer shares Customer Content to Axon in a support scenario, the Customer Content will be treated as Support Data but will only be used for resolving support incidents.

Axon may provide support through phone, email, or online chat. With Customer’s permission, Axon may use Guest Access (“GA") to temporarily navigate Customer’s Axon Cloud Service's tenant to view data in order to resolve a support incident. Phone conversations, online chat sessions, or GA sessions with Axon support professionals may be recorded and/or monitored.

Server and Data Location

CUSTOMER CONTENT

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



Axon ensures that all Customer Content in Axon Cloud Services 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 is located is in the United States and may be located in Customer's selected economic area for Customer Content.

Information Sharing

Axon may transfer data with its direct and indirect subsidiaries and Sub-processors, including, without limitation, service providers and other partners to support the overall delivery of Axon Products as described in “Data Collection and Processing Activities” section of this Policy.

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.

Customer consents to the transfer of Customer Content to Axon's Sub-processors for the purpose of storing Customer Content. Such Sub-processors responsible for storing Customer Content are contracted by Axon for data storage services. Ownership of Customer Content remains with Customer.

Axon may hire Sub-processors to provide or enhance Axon Products on its behalf. Axon will only permit any such Sub-processors to obtain Customer Content from Axon Cloud Services to deliver services to Axon and will be prohibited from using Customer Content for any other purpose. Axon may engage new Sub-processors. Axon will give Customer notice (by updating the website) of any new Sub-processor.

Prior to onboarding Sub-processors, Axon conducts an audit of the security and privacy practices of Sub-processors to ensure Sub-processors provide a level of security and privacy appropriate to its access to data and scope of services.

Under Privacy Shield's “Onward Transfer Principle”, Axon remains responsible for personal data that may be shared with Axon's Sub-processors.

Customer can transfer data from Axon Cloud Services to third parties. Customer must ensure data sharing agreements are in place with third parties to protect data throughout its lifecycle.

Axon Sub-Processors

Understand the server locations, data processed, and functions performed.
Axon maintains an up-to-date list of the names and locations of all Sub-processors. This list is below.

If you are a current Axon Cloud Services customer with a data processing agreement in place with

Axon, you may subscribe to receive notifications of a new Sub-processor(s) before Axon authorizes any new Sub-processor to process personal data in connection with the provision of your service.

You can subscribe to receive email notifications for changes to Axon Cloud Services Sub-processor(s) by submitting a request here.

For a complete list of Axon Sub-Processors, click here.

TELECOMMUNICATION SUB-PROCESSORS

Axon Body 3 includes embedded cellular technologies used to connect to telecommunication networks in order to provide connectivity between Axon Body 3 and Axon Cloud Services. Cellular technologies enable Axon Aware services. Customer's Axon Body 3 cameras will send data to the respective Axon Cloud Services region selected telecommunications providers as needed to enable cellular connectivity. Data includes Personal Data, such as location data. For Axon Body 3, Axon manages all cellular registration and account management associated to the cellular subscription. Personal Data of Customers is not collected by Axon or telecommunications providers for the purposes of cellular account management.

Outlined below is the telecommunication sub-processors. In regions where there are more than one telecommunication sub-processor, Axon will manage customers' Axon Body 3 cellular registration.

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*

Required Disclosures

Axon will not disclose Customer Content except as compelled by a court or administrative body or required by any law or regulation. Axon will notify Customer if any disclosure request is received for Customer Content so Customer may file an objection with the court or administrative body.

Customer's Access and Choice

Customer Content

Customer can access Customer's tenant to manage Customer Content.

Non-Content Data

Within the scope of Axon's authorization to do so, and in accordance with Axon's commitment under the Privacy Shield, Axon will work with Customers to provide access to Personal Data about Customer that Axon or Sub-processors holds. Axon will also take reasonable steps to enable Customers to correct, amend, or delete Personal Data that is demonstrated to be inaccurate.

If at any time after registering an account on Axon Cloud Services you desire to update Personal Data you have shared with us, change your mind about sharing Personal Data with us, desire to cancel your Customer account, or request that Axon no longer use provided Personal Data to provide you services, please contact us at privacy@axon.com. We will retain and use Personal Data for as long as needed to provide you services, comply with our legal obligations, resolve disputes, and enforce our agreements.

Certain data processing is determined by Customer based on Axon Product usage, Customer network or device configuration, and administrative settings made available with Axon Cloud Services or Axon Client Applications:

Axon Body 3 WiFi Positioning

Axon Body 3 cameras offer customers a feature to enhance location services where GPS/GNSS signals may not be available, for instance within buildings or underground. Customer administrators can manage their choice to use this service within the administrative features of Axon Cloud Services. When WiFi Positioning is enabled, Non-Content and Personal Data including location, device and network information data will be sent to Skyhook Holdings, Inc (Skyhook) to facilitate the WiFi Positioning functionality. Skyhook will act as both a data sub-processor (as reflected in this policy) and as a data controller. Skyhook becomes a data sub-processor for Axon when Skyhook processes data from Axon Body 3 devices to determine a location. Skyhook acts a data controller when it collects data sent from Axon Body 3 cameras to maintain their services and to develop new products, services or datasets. Data controlled by Skyhook is outside the scope of the Axon Cloud Services Privacy Policy and is subject to the Skyhook Services Privacy Policy.

Client Push Notifications

Axon Products leverage push notification services made available by mobile operating system providers (i.e. Google's Cloud Messaging and Apple's Push Notification Service to deliver functional notifications to client applications. Push notification services can be managed by leveraging notification settings made available in both mobile applications and the mobile operating system.

User Analytics

Customers can opt-out of user analytics tracking on Axon Cloud Services by disabling cookies or preventing Customer's browser or device from accepting new cookies. To prevent data from being collected by Mixpanel, network or device access to *.mixpanel.com should be blocked

Service Support

Mobile client application crash analytics are used provide Axon personnel insight to crashes when using Axon client applications. To opt out of crash reporting, network or device access to *.crashlytics.com should be blocked.

Geolocation Services

Geolocation services are critical to proper user functionality of many of Axon products. However, customers can chose to opt out of mapping and geolocation functionality by blocking network or device access to *.mapbox.com and *.arcgisonline.com

Data Security Measures

Axon is committed to help 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.

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 that Customer Data has been accessed, disclosed, altered, or destroyed by an unlawful or unauthorized party, Axon will notify relevant authorities and affected customers.

Within 48 hours of an incident confirmation, Axon will notify Customer administrators registered on Axon Cloud Services. Authorities will be notified through Axon's established channels and timelines. The notification will reasonably explain known facts, actions that have been taken, and make commitments regarding subsequent updates. Additional details are available in the Axon Cloud Services Security Incident Handling and Response Statement.

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 access to 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, may 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 Content will result in additional fees and Axon cannot warrant or guarantee data integrity or readability in the external systems.

Data Retention, Restitution, and Deletion

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 product and services

and in accordance with applicable regulations. As outlined below, Customer is responsible for adhering to its own retention policies and procedures.

Evidence Retention

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. Axon Cloud Services can automate weekly messages summarizing upcoming agency-wide deletions to all customer Axon Cloud Services administrators. Customer users can receive a weekly message regarding Evidence uploaded within their user account to protect against accidental deletions. Customer can recover Evidence up to 7 days after Customer queues such Evidence for deletion. After this 7-day grace period, Axon Cloud Services initiates deletion of Evidence. Data deletion processing may occur asynchronously across storage systems and data centers. During and after data deletion processing, Evidence will not be recovered or recoverable by any party.

Accountability

As outlined herein, Axon is committed to maintaining compliance with relevant security and privacy standards to ensure the continued security, availability, integrity, confidentiality, and privacy of Axon Cloud Services and Customer Data stored within.

In addition to the security efforts outlined herein, Axon will maintain its ISO/IEC 27001:2013 certification or comparable assurances for Axon Cloud Services. Customers may review the certificate.

Social Media Publishing

Axon provides social media features that enable Customer's and their end users ("Users") to share Customer Content directly from the Evidence Detail page in Axon Evidence to social media websites ("Publish to Social Media Feature"). For example: when a User uploads a video directly to YouTube from Axon Evidence. This may include Customer Content such as video, audio, images or other types of media or multimedia; and the title, description and tags associated with those media. Customer Axon Evidence administrators can manage the enablement of this feature, for all Users, within the administrative functions of Axon Evidence. The use of this feature by Users may result in the collection or sharing of information about them, depending on the feature. The privacy and security practices of the social media website is not covered by this Policy, and Axon is not responsible for, or makes attestations regarding, their privacy or security practices. When Users enable the Publish to Social Media Feature, and/or publish content to a social media website using this feature, they acknowledge and agree to be bound by the terms of service and privacy policy(s), if applicable, of the social media website in which the Customer Content is published to. Axon encourages Users to review the terms of service and privacy policy(s) of the social media website, to make sure they understand the data that may be collected, used, and shared by the website.

Google LLC, (YouTube API Services): Axon uses YouTube's API services in connection with our Publish to Social Media Feature. When Users link, connect, or login ("Connect") their Google

account(s) with Axon Evidence, they are agreeing to be bound by the YouTube Terms of Service (https://www.youtube.com/t/terms). In addition, they are directing Google to send Axon data as controlled by Google or as authorized by the User via their privacy settings at Google. Through YouTube's API services, Axon only accesses, collects, and stores a token which Axon uses to Connect the associated Google account(s) with Axon Evidence. The token is only used to enable a user to upload a video to YouTube and is not shared with external parties. Axon does not obtain or store the associated Google account(s) login credentials, through YouTube's API services.

Google has settings that list which apps can connect to a Google account(s). When Users Connect an associated Google account(s) to Axon Evidence, Axon Evidence gets authorized in these settings as a connected site or app. If Users remove Axon Evidence from these settings, its access to the account is revoked. Users may revoke this access at any time by following the instructions here: https://help.axon.com/hc/en-us/articles/360052689392-Removing-Axon-Evidence-Access-to-Your-YouTube-Account. Revoking Axon Evidence access will prevent Users from publishing videos to YouTube from Axon Evidence.

Axon encourages Users to review YouTube's Terms of Service (https://www.youtube.com/t/terms) and Google's Privacy Policy (http://www.google.com/policies/privacy) to make sure they understand the data that may be collected, used, and shared by Google.

Insurance

Axon will maintain, during the term of the Agreement, a cyber-insurance policy and will furnish certificates of insurance following Customer's written request.

How to Contact Us

Axon commits to resolve complaints about Customer privacy and use of Axon Products. Complaints surrounding this Policy can be directed to Customer's local Axon representative or privacy@axon.com. If Customer has any questions or concerns regarding privacy and security of Customer Content or Axon's handling of Customer's Personal Data under Privacy Shield, please contact privacy@axon.com.

If Customer is an EU citizen and we are unable to satisfactorily resolve any complaint relating to the Privacy Shield, or if Axon fails to acknowledge Customer's complaint in a timely fashion, Customer can contact the relevant EU Data Protection Authorities (DPAs) or the Swiss Federal Data Protection and Information Commissioner (FDPIC). In certain circumstances, the Privacy Shield provides the right to invoke binding arbitration to resolve complaints not resolved by other means, as described in Annex I to the Privacy Shield Principles in each of the Privacy Shield Frameworks. Axon is subject to the investigatory and enforcement powers of the U.S. Federal Trade Commission.

Axon Customer Experience Improvement Program Appendix

1. **Axon Customer Experience Improvement Program (ACEIP)**. Customer does not consent to participation in ACEIP at any level. Axon will not enroll Customer in its ACEIP program.

.

Professional Services Appendix

If any of the Professional Services specified below are included on the Quote, this Appendix applies.

1. **Utilization of Services**. Customer must use professional services as outlined in the Quote and this Appendix within six (6) months of the Effective Date.

2. **Axon Full Service (Axon Full Service)**. Axon Full Service includes advance remote project planning and configuration support and up to four (4) consecutive days of on-site service and a professional services manager to work with Customer to assess Customer's deployment and determine which on-site services are appropriate. If Customer requires more than four (4) consecutive on-site days, Customer must purchase additional days. Axon Full Service options include:

System set up and configuration • Instructor-led setup of Axon View on smartphones (if applicable) • Configure categories and custom roles based on Customer need • Register cameras to Customer domain • Troubleshoot IT issues with Axon Evidence and Axon Dock ("**Dock**") access • One on-site session included
Dock configuration • Work with Customer to decide the ideal location of Docks and set configurations on Dock • Authenticate Dock with Axon Evidence using admin credentials from Customer • On-site assistance, not to include physical mounting of docks
Best practice implementation planning session • Provide considerations for the establishment of video policy and system operations best practices based on Axon's observations with other agencies • Discuss the importance of entering metadata in the field for organization purposes and other best practices for digital data management • Provide referrals of other agencies using the Axon camera devices and Axon Evidence • Recommend rollout plan based on review of shift schedules
System Admin and troubleshooting training sessions Step-by-step explanation and assistance for Customer's configuration of security, roles & permissions, categories & retention, and other specific settings for Axon Evidence
Axon instructor training (Train the Trainer) Training for Customer's in-house instructors who can support Customer's Axon camera and Axon Evidence training needs after Axon has fulfilled its contractual on-site obligations
Evidence sharing training Tailored workflow instruction for Investigative Units on sharing Cases and Evidence with local prosecuting agencies
End user go-live training and support sessions • Assistance with device set up and configuration • Training on device use, Axon Evidence, and Evidence Sync
Implementation document packet Axon Evidence administrator guides, camera implementation guides, network setup guide, sample policies, and categories & roles guide
Post go-live review

3. **Body-Worn Camera Starter Service (Axon Starter)**. Axon Starter includes advance remote project planning and configuration support and one (1) day of on-site Services and a professional services manager to work closely with Customer to assess Customer's deployment and determine which Services are appropriate. If Customer requires more than one (1) day of on-site Services, Customer must purchase additional on-site Services. The Axon Starter options include:

System set up and configuration (Remote Support)

• Instructor-led setup of Axon View on smartphones (if applicable) • Configure categories & custom roles based on Customer need • Troubleshoot IT issues with Axon Evidence and Dock access
Dock configuration • Work with Customer to decide the ideal location of Dock setup and set configurations on Dock • Authenticate Dock with Axon Evidence using "Administrator" credentials from Customer • Does not include physical mounting of docks
Axon instructor training (Train the Trainer) Training for Customer's in-house instructors who can support Customer's Axon camera and Axon Evidence training needs after Axon's has fulfilled its contracted on-site obligations
End user go-live training and support sessions • Assistance with device set up and configuration • Training on device use, Axon Evidence, and Evidence Sync
Implementation document packet Axon Evidence administrator guides, camera implementation guides, network setup guide, sample policies, and categories & roles guide

4. **Body-Worn Camera Virtual 1-Day Service (Axon Virtual)**. Axon Virtual includes all items in the BWC Starter Service Package, except one (1) day of on-site services.

5. **CEW Services Packages**. CEW Services Packages are detailed below:

System set up and configuration • Configure Axon Evidence categories & custom roles based on Customer need. • Troubleshoot IT issues with Axon Evidence. • Register users and assign roles in Axon Evidence. • **For the CEW Full Service Package**: On-site assistance included • **For the CEW Starter Package**: Virtual assistance included
Dedicated Project Manager Assignment of specific Axon representative for all aspects of planning the rollout (Project Manager). Ideally, Project Manager will be assigned to Customer 4–6 weeks before rollout
Best practice implementation planning session to include: • Provide considerations for the establishment of CEW policy and system operations best practices based on Axon's observations with other agencies • Discuss the importance of entering metadata and best practices for digital data management • Provide referrals to other agencies using TASER CEWs and Axon Evidence • **For the CEW Full Service Package:** On-site assistance included • **For the CEW Starter Package:** Virtual assistance included
System Admin and troubleshooting training sessions On-site sessions providing a step-by-step explanation and assistance for Customer's configuration of security, roles & permissions, categories & retention, and other specific settings for Axon Evidence
Axon Evidence Instructor training • Provide training on the Axon Evidence to educate instructors who can support Customer's subsequent Axon Evidence training needs. • **For the CEW Full Service Package:** Training for up to 3 individuals at Customer • **For the CEW Starter Package:** Training for up to 1 individual at Customer
TASER CEW inspection and device assignment Axon's on-site professional services team will perform functions check on all new TASER CEW Smart weapons and assign them to a user on Axon Evidence.
Post go-live review **For the CEW Full Service Package**: On-site assistance included. **For the CEW Starter Package**: Virtual assistance included.

6. **Smart Weapon Transition Service**. The Smart Weapon Transition Service includes:

Archival of CEW Firing Logs Axon's on-site professional services team will upload CEW firing logs to Axon Evidence from all TASER CEW

Smart Weapons that Customer is replacing with newer Smart Weapon models.
Return of Old Weapons Axon's on-site professional service team will ship all old weapons back to Axon's headquarters. Axon will provide Customer with a Certificate of Destruction

*Note: CEW Full Service packages for TASER 7 or TASER 10 include Smart Weapon Transition Service instead of 1-Day Device Specific Instructor Course.

7. **VR Services Package.** VR Service includes advance remote project planning and configuration support and one (1) day of on-site service and a professional services manager to work with Customer to assess Customer's deployment and determine which Services are appropriate. The VR Service training options include:

System set up and configuration (Remote Support) • Instructor-led setup of Axon VR headset content • Configure Customer settings based on Customer need • Troubleshoot IT issues with Axon VR headset
Axon instructor training (Train the Trainer) Training for up to five (5) Customer's in-house instructors who can support Customer's Axon VR CET and SIM training needs after Axon's has fulfilled its contracted on-site obligations
Classroom and practical training sessions Step-by-step explanation and assistance for Customer's configuration of Axon VR CET and SIM functionality, basic operation, and best practices

8. **Axon Air, On-Site Training.** Axon Air, On-Site training includes advance remote project planning and configuration support and one (1) day of on-site Services and a professional services manager to work closely with Customer to assess Customer's deployment and determine which Services are appropriate. If Customer's requires more than one (1) day of on-site Services, Customer must purchase additional on-site Services. The Axon Air, On-Site training options include:

System set up and configuration (Remote Support) • Instructor-led setup of Axon Air App (ASDS) • Configure Customer settings based on Customer need • Configure drone controller • Troubleshoot IT issues with Axon Evidence
Axon instructor training (Train the Trainer) Training for Customer's in-house instructors who can support Customer's Axon Air and Axon Evidence training needs after Axon's has fulfilled its contracted on-site obligations
Classroom and practical training sessions Step-by-step explanation and assistance for Customer's configuration of Axon Respond+ livestreaming functionality, basic operation, and best practices

9. **Axon Air, Virtual Training.** Axon Air, Virtual training includes all items in the Axon Air, On-Site Training Package, except the practical training session, with the Axon Instructor training for up to four hours virtually.

10. **Signal Sidearm Installation Service**.

    a. **Purchases of 50 SSA units or more**: Axon will provide one (1) day of on-site service and one professional services manager and will provide train the trainer instruction, with direct assistance on the first of each unique holster/mounting type. Customer is responsible for providing a suitable work/training area.

    b. **Purchases of less than 50 SSA units:** Axon will provide a 1-hour virtual instruction session on the basics of installation and device calibration**.**

11. **Out of Scope Services**. Axon is only responsible to perform the professional services described in the Quote and this Appendix. Any additional professional services are out of scope. The Parties must document scope changes in a written and signed amendment in accordance with Article 10(c) of the Professional Services Agreement.

12. **Delivery of Services**. Axon personnel will work Monday through Friday, 8:30 a.m. to 5:30 p.m., except holidays. Axon will perform all on-site tasks over a consecutive timeframe. Axon will not charge Customer travel time by Axon

personnel to Customer premises as work hours.

13. **Access Computer Systems to Perform Services**. Customer authorizes Axon to access relevant Customer computers and networks, solely for performing the Services. Axon will work to identify as soon as reasonably practicable resources and information Axon expects to use and will provide an initial itemized list to Customer. Customer is responsible for and assumes the risk of any problems, delays, losses, claims, or expenses resulting from the content, accuracy, completeness, and consistency of all data, materials, and information supplied by Customer.

14. **Site Preparation**. Axon will provide a hardcopy or digital copy of current user documentation for the Axon Devices ("**User Documentation**"). User Documentation will include all required environmental specifications for the professional services and Axon Devices to operate per the Axon Device User Documentation. Before installation of Axon Devices (whether performed by Customer or Axon), Customer must prepare the location(s) where Axon Devices are to be installed ("**Installation Site**") per the environmental specifications in the Axon Device User Documentation. Following installation, Customer must maintain the Installation Site per the environmental specifications. If Axon modifies Axon Device User Documentation for any Axon Devices under this Agreement, Axon will provide the update to Customer when Axon generally releases it

15. **Acceptance**. When Axon completes professional services, if Customer reasonably believes Axon did not complete the professional services in substantial conformance with this Agreement, excluding latent defects, Customer must notify Axon in writing of the specific reasons for rejection within thirty (30) calendar days from delivery of the Acceptance Form. Axon will address the issues . If Axon does not receive written notification of reasons for rejection within thirty (30) calendar days of delivery, excluding latent defects, Axon will deem Customer to have accepted the professional services.

16. **Customer Network**. For work performed by Axon transiting or making use of Customer's network, Customer is solely responsible for maintenance and functionality of the network. In no event will Axon be liable for loss, damage, or corruption of Customer's network from any cause excluding loss, damage, or corruption caused by Axon.

Technology Assurance Plan Appendix

[Deleted]

TASER Device Appendix

[Deleted]

Axon Auto-Tagging Appendix

[Deleted]

Axon Respond Appendix

[Deleted]

Add-on Services Appendix

This Appendix applies if Axon Community Request, Axon Redaction Assistant, and/or Axon Performance are included on the Quote.

1. **Subscription Term**. If Customer purchases Axon Community Request, Axon Redaction Assistant, or Axon Performance as part of OSP 7 or OSP 10, the subscription begins on the later of the (1) start date of the OSP 7 or OSP 10 Term, or (2) date Axon provisions Axon Community Request Axon Redaction Assistant, or Axon Performance to Customer.

   1.1. If Customer purchases Axon Community Request, Axon Redaction Assistant, or Axon Performance as a standalone, the subscription begins the later of the (1) date Axon provisions Axon Community Request, Axon Redaction Assistant, or Axon Performance to Customer, or (2) first day of the month following the Effective Date.

   1.2. The subscription term will end upon the completion of the Axon Evidence Subscription associated with the add-on.

2. **Axon Community Request Storage**. For Axon Community Request, Customer may store an unlimited amount of data submitted through the public portal ("**Portal Content**"), within Customer's Axon Evidence instance. The post-termination provisions outlined in the Axon Cloud Services Terms of Use Appendix also apply to Portal Content.

3. **Performance Auto-Tagging Data**. In order to provide some features of Axon Performance to Customer, Axon will need to store call for service data from Customer's CAD or RMS.

Axon Application Programming Interface Appendix

This Appendix applies if Axon's API Services or a subscription to Axon Cloud Services is 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 may 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 viruses, worms, defect, Trojan horses, malware, or any items 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 Investigate Appendix

If the Quote includes Axon's On Prem Video Suite known as Axon Investigate or Third Party Video Support License, the following appendix shall apply.

1. **License Grant**. Subject to the terms and conditions specified below and upon payment of the applicable fees set forth in the Quote, Axon grants to Customer a nonexclusive, nontransferable license to install, use, and display the Axon Investigate software ("**Software**") solely for its own internal use only and for no other purpose, for the duration of subscription term set forth in the Quote. This Agreement does not grant Customer any right to enhancements or updates, but if such are made available to Customer and obtained by Customer they shall become part of the Software and governed by the terms of this Agreement.

2. **Third-Party Licenses**. Axon licenses several third-party codecs and applications that are integrated into the Software. Users with an active support contract with Axon are granted access to these additional features. By accepting this agreement, Customer agrees to and understands that an active support contract is required for all of the following features: DNxHD output formats, decoding files via the "fast indexing" method, proprietary file metadata, telephone and email support, and all future updates to the software. If Customer terminates the annual support contract with Axon, the features listed above will be disabled within the Software. It is recommended that users remain on an active support contract to maintain the full functionality of the Software.

3. **Restrictions on Use**. Customer may not permit any other person to use the Software unless such use is in accordance with the terms of this Agreement. Customer may not modify, translate, reverse engineer, reverse compile, decompile, disassemble or create derivative works with respect to the Software, except to the extent applicable laws specifically prohibit such restrictions. Customer may not rent, lease, sublicense, grant a security interest in or otherwise transfer Customer's rights to or to use the Software. Any rights not granted are reserved to Axon.

4. **Term**. For purchased perpetual Licenses only—excluding Licenses leased for a pre-determined period, evaluation licenses, companion licenses, as well as temporary licenses--the license shall be perpetual unless Customer fails to observe any of its terms, in which case it shall terminate immediately, and without additional prior notice. The terms of Paragraphs 1, 2, 3, 5, 6, 8 and 9 shall survive termination of this Agreement. For licenses leased for a pre-determined period, for evaluation licenses, companion licenses, as well as temporary licenses, the license is granted for a period beginning at the installation date and for the duration of the evaluation period or temporary period as agreed between Axon and Customer.

5. **Title**. Axon and its licensors shall have sole and exclusive ownership of all right, title, and interest in and to the Software and all changes, modifications, and enhancements thereof (including ownership of all trade secrets and copyrights pertaining thereto), regardless of the form or media in which the original or copies may exist, subject only to the rights and privileges expressly granted by Axon. This Agreement does not provide Customer with title or ownership of the Software, but only a right of limited use.

6. **Copies**. The Software is copyrighted under the laws of the United States and international treaty provisions. Customer may not copy the Software except for backup or archival purposes, and all such copies shall contain all Axon's notices regarding proprietary rights as contained in the Software as originally provided to Customer. If Customer receives one copy electronically and another copy on media, the copy on media may be used only for archival purposes and this license does not authorize Customer to use the copy of media on an additional server.

7. **Actions Required Upon Termination**. Upon termination of the license associated with this Agreement, Customer agrees to destroy all copies of the Software and other text and/or graphical documentation, whether in electronic or printed format, that describe the features, functions and operation of the Software that are provided by Axon to Customer ("**Software Documentation**") or return such copies to Axon. Regarding any copies of media containing regular backups of Customer's computer or computer system, Customer agrees not to access such media for the purpose of recovering the Software or online Software Documentation. Notwithstanding the foregoing, the County may take any action necessary to comply with the requirements of the Local Records Act (50 ILCS 205, et. seq.), or the Illinois Freedom of Information Act (5 ILCS 140, et seq.)

8. **Export Controls**. None of the Software, Software Documentation or underlying information may be downloaded or otherwise exported, directly or indirectly, without the prior written consent, if required, of the office of Export Administration of the United States, Department of Commerce, nor to any country to which the U.S. has embargoed goods, to any person on the U.S. Treasury Department's list of Specially Designated Nations, or the U.S. Department of Commerce's Table of Denials.

9. **U.S. Government Restricted Rights**. The Software and Software Documentation are Commercial Computer Software provided with Restricted Rights under Federal Acquisition Regulations and Customer supplements to them.

Use, duplication or disclosure by the U.S. Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFAR 255.227-7013 et. Seq. or 252.211-7015, or subparagraphs (a) through (d) of the Commercial Computer Software Restricted Rights at FAR 52.227-19, as applicable, or similar clauses in the NASA FAR Supplement. Contractor/manufacturer is Axon Enterprise, Inc., 17800 North 85th Street, Scottsdale, Arizona 85255.

AI Technology Appendix

This AI Technology Appendix shall only apply to Customers who license Axon Cloud Services in a Quote that specifically utilizes AI Technology. Unless explicitly defined otherwise, capitalized terms used in this Appendix have the same meaning as those in the Agreement.

1. Definitions.

   1.1. **AI Technology.** Refers to artificial intelligence functionalities embedded in Axon's Cloud Services, which may include: (a) Enhanced Evidence Management; (b) AI-powered redaction tools; (c) Large Language Model-based tools (e.g., "Draft One" "Policy Chat"); (d) Predictive Analytics for operational insights; or (e) Natural Language Processing (NLP) for text and speech analysis.

   1.2. **Model Drift.** The degradation of AI model performance due to changes in input data or external conditions, requiring retraining or updates.

   1.3. **Bias Mitigation.** Strategies and techniques used to identify, measure, and minimize bias in AI Technology.

2. Scope and Usage.

   2.1. **Integration.** Axon AI Technology is intended to improve public safety, streamline operations, and ensure data accuracy. The AI functionalities will only be used as described in the Agreement or applicable documentation.

   2.2. **Data Use.** Axon acts as a Data Processor for AI Technology. All inquiries submitted are processed solely to provide accurate responses based on Customer Content submitted. Customer remains the Data Controller of all Customer Content. Axon and Axon's subprocessors do not train their models on Customer Content. Customers who elect to participate in Axon's ACEIP program can enter into custom agreements to assist in product development efforts like AI model training. Even in those cases, Axon operates carefully on redacted data and not on Customer Content.

   2.3. **Automatic Data Collection.** AI Technology may automatically collect Non-Content Data about user interactions with the service and their devices to enhance the functionality and security of the system. The details collected include, but are not limited to, the following:

      2.3.1. **User Engagement and Activity Metrics.** AI Technology may track key engagement statistics, including Daily Active Users (DAUs), Weekly Active Users (WAUs), and Monthly Active Users (MAUs). Additional metrics include new user activations, repeat usage rates, total queries submitted, follow-up query volume, session lengths, retention rates, and user satisfaction ratings (e.g., thumbs up/down feedback).

      2.3.2. **Sales and Adoption Tracking.** Axon monitors the number of licenses and agencies purchasing the service, including those in trial phases, fully deploying the service, and conversion rates from trials to paid subscriptions.

      2.3.3. **End User inputs.** Axon may process de-identified end-user inputs to the AI Technology, excluding Customer Content or any data that directly or indirectly identifies individuals.

3. Axon Responsibilities.

   3.1. **Ethical AI Development.** Axon shall: (a) Follow its responsible innovation framework; (b) Engage with the Ethics and Equity Advisory Council (EEAC) for feedback; (c) Conduct testing to minimize bias and ensure reliability; and (d) Implement Bias Mitigation techniques in model development and deployment.

   3.2. **Security Program.** Axon will maintain a comprehensive information security program, including logical and physical access, vulnerability, risk, and configuration management; incident monitoring and response; encryption of digital evidence; and security education.

   3.3. **Transparency.** Axon will provide documentation describing AI functionalities and their intended use and disclose any material limitations, risks, or Model Drift incidents.

   3.4. **Incident Response.** Axon will promptly address and rectify anomalies in AI functionalities, as outlined in its incident management procedures.

   3.5. **Compliance.** Axon will ensure compliance with applicable laws, regulations, and standards, including but not limited to the EU AI Act, NIST AI standards, and ISO/IEC 27001.

4. Customer Responsibilities.

   4.1. **Ownership of Customer Content.** Customer controls and owns all rights, title, and interest in Customer Content. Axon obtains no interest in Customer Content and will only access Customer Content for limited purposes as outlined in the Agreement.

   4.2. **Use of AI Technologies.** Customer must: (a) review AI-generated outputs to ensure accuracy and appropriateness; (b) maintain control over Customer Content shared with AI Technologies (c) comply with applicable laws when using Axon AI Technology and Axon Services; (d) monitor for potential issues with AI outputs, including false positives or negatives; and (e) provide timely feedback on Axon AI Technology performance.

   4.3. **Restrictions.** AI Technology is not designed for emergencies, and in such cases, users should contact appropriate emergency services directly. Axon disclaims liability for queries containing prohibited content, such as hate, sexual material, or violence, and reserves the right to restrict such usage.

5. Policy Chat. This section outlines the specific terms and conditions related to the use of Policy Chat by the Customer. By utilizing Policy Chat, the Customer agrees to comply with the following provisions:

   5.1. **License and Content Restrictions.** Any uploads beyond 5,000 pages may be limited by Axon. It is the Customer's responsibility to manage uploads to ensure system efficiency and compliance with these terms.

   5.2. **Data Processing.** Inquiries submitted to Policy Chat are processed solely to provide accurate responses based on existing policy documents provided by the Customer. The Customer remains the Data Controller of all policy content, and Axon's role is strictly limited to facilitating access to this information through Policy Chat.

   5.3. **Policy Chat Restrictions.** The information provided by Policy Chat is for informational purposes only and is based on the policy documents uploaded by the Customer. **Axon does not guarantee the accuracy, completeness, or timeliness of the information, and disclaims all liability for any reliance placed on such information**. Policy Chat is not a substitute for official policy documents, legal advice, or comprehensive training. Users should consult their supervisors, legal advisors, or official sources for the most accurate and up-to-date policy guidance. Changes to policies may not be reflected immediately, and it is the Customer's responsibility to ensure data integrity by uploading the most current documents and removing outdated versions.

6. **Draft One.** Specifically for Customers who utilize Draft One, Axon may impose usage restrictions if a single user generates more than three hundred (300) reports per month for two or more consecutive months.

7. Brief One. Brief One includes automatic summarization of all products that can be transcribed. If Customer subscribes to Brief One, Customer may utilize Brief One with no limit on the number of pieces of evidence or cases. Notwithstanding the foregoing, Axon may limit evidence and case summaries for cases with over one thousand (1000) pieces of evidence or after three hundred (300) cases per End User per month for two (2) consecutive months in a row.

8. Auto-Transcribe. This section outlines licensing terms for Customer's subscription of Auto-Transcribe:

   8.1. **A-La-Carte Minutes.** Upon Axon granting Customer a set number of minutes, Customer may utilize Axon Auto-Transcribe, subject to the number of minutes allowed on the Quote. Customers cannot roll over unused minutes to future Auto-Transcribe terms. Axon may charge Customer additional fees for exceeding the number of purchased minutes. Axon Auto-Transcribe minutes expire one year after being provisioned to Customer by Axon.

   8.2. **Axon Unlimited Transcribe.** Upon Axon granting Customer an Unlimited Transcribe subscription to Axon Auto-Transcribe, Customer may utilize Axon Auto-Transcribe with no limit on the number of minutes. Unlimited Transcribe includes automatic transcription of all Axon BWC and Axon Capture footage. With regard to Axon Interview Room, Axon Fleet, Axon Community Request, or third-party transcription, transcription must be requested on demand. Notwithstanding the foregoing, Axon may limit usage after 5,000 minutes per user per month for multiple months in a row. Axon will not bill for overages.

Axon Technical Account Manager Appendix

This Appendix applies if Axon Support Engineer services are included in the Quote.

1. **Axon Technical Account Manager Payment.** Axon will invoice for Axon Technical Account Manager ("**TAM**") services, as outlined in the Quote, when the TAM commences work on-site at Customer.

2. **Full-Time TAM Scope of Services.**

   2.1. A Full-Time TAM will work on-site four (4) days per week, unless an alternate schedule or reporting location is mutually agreed upon by Axon and Customer.

   2.2. Customer's Axon sales representative and Axon's Customer Success team will work with Customer to define its support needs and ensure the Full-Time TAM has skills to align with those needs. There may be up to a six- (6-) month waiting period before the Full-Time TAM can work on-site, depending upon Customer's needs and availability of a Full-Time TAM.

   2.3. The purchase of Full-Time TAM Services includes two (2) complimentary Axon Accelerate tickets per year of the Agreement, so long as the TAM has started work at Customer, and Customer is current on all payments for the Full-Time TAM Service.

   2.4. The Full-Time TAM **Service options are listed below:**

Ongoing System Set-up and Configuration Assisting with assigning cameras and registering docks Maintaining **Customer's Axon Evidence account** Connecting Customer to "Early Access" programs for new devices
Account Maintenance Conducting on-site training on new features and **devices for Customer leadership team(s)** Thoroughly documenting issues and workflows and suggesting new workflows to improve **the effectiveness of the Axon program** Conducting weekly meetings to cover current issues and program status
Data Analysis Providing on-demand Axon usage data to identify trends and insights for improving daily workflows Comparing **Customer's Axon usage and trends to peers to establish best practices** Proactively monitoring the health of Axon equipment and coordinating returns when needed
Direct Support Providing on-site, Tier 1 and Tier 2 (as defined in Axon's Service Level Agreement) technical support for Axon Devices Proactively monitoring the health of **Axon equipment** Creating and monitoring RMAs **on-site** Providing Axon app support Monitoring and testing new firmware and workflows before they are released to Customer's production environment
Customer Advocacy Coordinating bi-**annual voice of customer meetings with Axon's Device Management team** Recording and tracking Customer feature requests and major bugs

3. **Regional TAM Scope of Services.**

   3.1. A Regional TAM will work on-site for three (3) consecutive days per quarter. Customer must schedule the on-site days at least two (2) weeks in advance. The Regional TAM will also be available by phone and email during regular business hours up to eight (8) hours per week.

   3.2. There may be up to a six- (6-) month waiting period before Axon assigns a Regional TAM to Customer, depending upon the availability of a Regional TAM.

   3.3. The purchase of Regional TAM Services includes two (2) complimentary Axon Accelerate tickets per year of the Agreement, so long as the TAM has started work at Customer and Customer is current on all payments for the Regional TAM Service.

   3.4. The Regional TAM service options are listed below:

Account Maintenance Conducting remote training on new features and **devices for Customer's leadership** Thoroughly documenting issues and workflows and suggesting new **workflows to improve the effectiveness of the Axon program** Conducting weekly conference calls to cover **current issues and program status** Visiting Customer quarterly (up to 3 consecutive days) to perform a quarterly business review, discuss Customer's goals for your Axon program, and continue to ensure a successful deployment of Axon Devices
Direct Support **Providing remote, Tier 1 and Tier 2 (As defined Axon's Service Level Agreement) technical support for Axon Devices** Creating and monitoring RMAs remotely
Data Analysis Providing quarterly Axon **usage data to identify trends and program efficiency opportunities** Comparing **Customer's Axon usage and trends to peers to establish best practices** Proactively monitoring the health of Axon equipment and coordinating returns when needed
Customer Advocacy Coordinating bi-yearly Voice of **Customer meetings with Device Management team** Recording and tracking Customer feature requests and major bugs

4. **Out of Scope Services.** The TAM is responsible to perform only the Services described in this Appendix. Any additional Services discussed or implied that are not defined explicitly in this Appendix will be considered out of the scope.
5. **TAM Leave Time.** The TAM will be allowed up to seven (7) days of sick leave and up to fifteen (15) days of vacation time per each calendar year. The TAM will work with Customer to coordinate any time off and will provide Customer with at least two (2) weeks' notice before utilizing any vacation days.

Axon Channel Services Appendix

This Appendix applies if Customer purchases Axon Channel Service, as set forth on the Quote.

1. **Definitions**.

   1.1. "**Axon Digital Evidence Management System**" means Axon Evidence or Axon Evidence Local, as specified in the attached Channel Services Statement of Work.

   1.2. "**Active Channel**" means a third-party system that is continuously communicating with an Axon Digital Evidence Management System.

   1.3. "**Inactive Channel**" means a third-party system that will have a one-time communication to an Axon Digital Evidence Management System.

2. **Scope.** Customer currently has a third-party system or data repository from which Customer desires to share data with Axon Digital Evidence Management. Axon will facilitate the transfer of Customer's third-party data into an Axon Digital Evidence Management System or the transfer of Customer data out of an Axon Digital Evidence Management System as defined in the Channel Services Statement of Work ("**Channel Services SOW**"). Channel Services will not delete any Customer Content. Customer is responsible for verifying all necessary data is migrated correctly and retained per Customer policy.

3. **Changes.** Axon is only responsible to perform the Services described in this Appendix and Channel Services SOW. Any additional services are out of scope. The Parties must document scope changes in a written and signed change order. Changes may require an equitable adjustment in the charges or schedule.

4. **Purpose and Use.** Customer is responsible for verifying Customer has the right to share data from and provide access to third-party system as it relates to the Services described in this Appendix and the Channel Services SOW. For Active Channels, Customer is responsible for any changes to a third-party system that may affect the functionality of the channel service. Any additional work required for the continuation of the Service may require additional fees. An Axon Field Engineer may require access to Customer's network and systems to perform the Services described in the Channel Services SOW. Customer is responsible for facilitating this access per all laws and policies applicable to Customer.

5. **Project Management.** Axon will assign a Project Manager to work closely with Customer's project manager and project team members and will be responsible for completing the tasks required to meet all contract deliverables on time and budget.

6. **Warranty.** Axon warrants that it will perform the Channel Services in a workmanlike manner.

7. **Monitoring.** Axon may monitor Customer's use of Channel Services to ensure quality, improve Axon devices and services, prepare invoices based on the total amount of data migrated, and verify compliance with this Agreement. Customer agrees not to interfere with such monitoring or obscure from Axon Customer's use of channel services.

8. **Customer's Responsibilities.** Axon's successful performance of the Channel Services requires Customer:

   8.1. Make available its relevant systems for assessment by Axon (including making these systems available to Axon via remote access);

   8.2. Provide access to the building facilities and where Axon is to perform the Channel Services, subject to safety and security restrictions imposed by the Customer (including providing security passes or other necessary documentation to Axon representatives performing the Channel Services permitting them to enter and exit Customer premises with laptop personal computers and any other materials needed to perform the Channel Services);

   8.3. Provide all necessary infrastructure and software information (TCP/IP addresses, node names, and network configuration) for Axon to provide the Channel Services;

   8.4. Ensure all appropriate data backups are performed;

   8.5. Provide Axon with remote access to the Customer's network and third-party systems when required for Axon to perform the Channel Services;

   8.6. Notify Axon of any network or machine maintenance that may impact the performance of the Channel Services; and

   8.7. Ensure the reasonable availability by phone or email of knowledgeable staff, personnel, system administrators, and operators to provide timely, accurate, complete, and up-to-date documentation and information to Axon (these contacts are to provide background information and clarification of information required to perform the Channel Services).

EXHIBIT 4

Cook County Information Technology and Data Special Conditions (ITDSC)

Cook County Government
Information Technology and Data Special Conditions Addendum

Together the Professional Services Agreement ("PSA") Cook County contract (#2526-10211), including any attachments thereto, and this Information Technology and Data Special Conditions Addendum ("Addendum"), form the "Agreement." County and Consultant agree that, with respect to County Data and/or County Intellectual Property, including any Consultant obligations, representation, or warranties related thereto, in the event of conflict between this Addendum and any other terms in the Agreement, this Addendum takes precedent over, controls and supersedes any term or clause to the contrary.

I. Definitions

a. "**AI System(s)**" means a machine-based framework that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions influencing physical or virtual environments. "AI System" includes machine-based frameworks utilizing generative pre-trained transformers and large language models.

b. **"Applicable Data Security and Privacy Law(s)"** means any applicable and relevant US laws, regulations, industry self-regulatory standards, and codes of practice in connection with the processing of Personally Identifiable Information, including but not limited to the Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. § 1320(d) et seq.); the Health Information Technology for Economic and Clinical Health Act of 2009 (42 U.S.C. § 17921 et seq.); FBI CJIS Security Policy; the Illinois Biometric Privacy Act, 740 ILCS 14/1, et seq.; the Illinois Personal Information Protection Act, 815 ILCS 530/1, et seq.; the Payment Card Industry Data Security Standard, including any subsequent updates, amendments and implementing regulations to the above laws, that may be applicable to the provision of the Services, Software, use of AI System, and/or this Agreement.

c. "**Biometric Identifier**" means a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry, and includes any expansion of this definition as enacted by the relevant legislative body and/or related case law. Additionally, photographs, videos, and voice recordings are included only to the extent utilized to capture such scans or prints.

d. "**Biometric Information**" means any information, regardless of how captured, converted, stored, or shared, based on an individual's Biometric Identifier that is used to identify an individual. Biometric information does not include information derived from items or procedures excluded under the definition of Biometric Identifiers. Biometric Information includes the most recent meaning or binding

judicial interpretation of the term "biometric information" as defined in the Illinois Biometric Privacy Act, 740 ILCS 14/10.

e. "**Business Associate Agreement**" means an agreement that meets the requirements of 45 C.F.R. 164.504(e).

f. "**Cardholder Data**" means data that meets the definition of "Cardholder Data" in the most recent Payment Card Industry Data Security Standard.

g. "**Consultant**" means the same as "Contractor" and "Axon" as both terms are defined in County Professional Services Agreement, or as defined in County Instruction to Bidders and General Conditions, if either document forms the basis of this Agreement. "Contractor" and "Consultant" may be interchangeably used. "Consultant" includes employees, representatives, subcontractors, and agents of Consultant.

h. "**Consultant Confidential Information**" means all non-public proprietary information of Consultant that is marked confidential, restricted, proprietary, or with a similar designation, provided that Consultant Confidential Information excludes County Data or information that may be subject to disclosure under Illinois Freedom of Information Act, 5 ILCS 140/1 et seq. or other law.

i. "**County**" has the same meaning as defined in the Cook County Procurement Code, located at Chapter 1, Sec. 1-3, of the Cook County Code of Ordinances as amended.

j. "**County Confidential Information**" means all non-public proprietary information of the County, including Personally Identifiable Information and any information exempt from public disclosure under the Illinois Freedom of Information Act, 5 ILCS 140/1 et seq. or under the Cook County Code of Ordinances. All Confidential Information is contained within the definition of Customer Content.

k. **"County Data"** means any and all information, in any form, that the County provides access to or shares with Consultant.

County Data also includes, without limitation, all information provided by County employees and representatives, as well as information provided by any third party on the County's behalf, to Consultant, and any information owned, created, and/or maintained by County that Consultant encounters during the term of this Agreement.

County Data does not include any data or intellectual property owned or created by Consultant, including proprietary or trade secret data, except for any data or intellectual property that the County is commissioning or purchasing from Consultant or that Consultant has been hired to create for the County.

l. "**County Intellectual Property**" or "**County IP**" means all Intellectual Property owned or licensed by the County, including Developed IP.

m. "**Criminal Justice Agency(ies)**" means a court, governmental agency (federal, state, local or tribal), or any subunit of governmental agency, that administers criminal justice pursuant to a statute or executive order and allocates a substantial part of its annual budget to administering criminal justice. Criminal Justice Agency includes state and federal Inspector General Offices and Sheriff's Offices.

n. "**Criminal Justice Information**" or "**CJIS Information**" means data or information, in virtual or hard copy form, collected by Criminal Justice Agencies regarding individuals consisting of identifiable descriptions and notations of arrests, detentions, indictments, informations, or other formal criminal charges, and any disposition arising therefrom, including acquittal, sentencing, correctional supervision, and release. The term does not include identification information such as fingerprint records if such information does not indicate the individual's involvement with the criminal justice system.

Criminal Justice Information also means any data that meets the definition of "Criminal Justice Information" in the most recent version of FBI CJIS Security Policy as well as data that meets the definition of "Criminal History Record Information" at 28 C.F.R. 20.

o. "**Cyber Incident**" means an occurrence of any kind that is reasonably likely to threaten or compromise, or does threaten or compromise, the security, integrity, availability, and confidentiality of, or access to, an information system, computer system, and/or the cyber security tools, controls, or procedures put in place to secure Consultant's systems, endpoints, servers, and/or its cloud environment, and has the potential to cause a Data Breach. Cyber Incident includes, but is not limited to, a ransomware event; a large scale failure of Consultant's Information Security System; any configuration problems which cause data to be stored or shared in violation of either Consultant's or Consultant's Third Party Vendor's Information Security Program; and any mistake or unintentional issue that causes cybersecurity protections to fail or otherwise not protect County Data and/or allows for the unauthorized access to or exfiltration of County Data.

p. **"Data Breach"** means (a) the loss or misuse (by any means) of any County Confidential Information; (b) the unauthorized or unlawful access, use, modification, destruction, corruption, or disclosure of any County Confidential Information; or (c) any other act or omission that compromises the security, confidentiality, integrity, or availability of any County Confidential Information.

q. **"Data Subject"** and any variation of that word mean the same as defined in Applicable Data Security and Privacy Laws.

r. **"Data Subject Request"** means a request made by a Data Subject to exercise any rights of Data Subjects under the Applicable Data and Security Privacy Laws.

s. "**Deliverable**" means the same as defined in the Professional Services Agreement or as defined in County Instruction to Bidders and General Conditions, if either document forms the basis of this Agreement.

t. "**Developed Intellectual Property"** or **"Developed IP"** means Intellectual Property conceived, developed, authored, or reduced to practice in the course of or in connection with the provision of the Services, including, but not limited to: (a) modifications to, or enhancements (derivative works) of, the County IP; (b) Developed Software; and (c) modifications to, or enhancements (derivative works) of, third party Intellectual Property to the extent not owned by the licensor of the third party IP under the terms of the applicable license.

u. "**Evolution Data**" means data created by, incorporated into, and a component of the AI System's evolution during training and subsequent use by County during the Term, including retained portions of any training data, production data, or Output Data as provided, directly or indirectly, by County.

v. "**Information Security Program**" means a detailed set of policies, procedures, and principles that describe how an organization protects its data and systems from unauthorized access, use, disclosure, disruption, modification, or destruction.

w. "**Input Data**" means data, regardless of form, that is entered into an AI System for processing.

x. "**Open Source Materials**" means any Software that: (a) contains, or is derived in any manner (in whole or in part) from, any Software distributed as free Software, open source Software, shareware (e.g., Linux), or similar licensing or distribution models; and (b) is subject to any agreement with terms requiring that such Software be (i) disclosed or distributed in source code or object code form, (ii) licensed for the purpose of making derivative works, and/or (iii) redistributable. Open Source Materials includes without limitation "open source" code as defined by the Open Source Initiative and "free" code as defined by the Free Software Foundation.

y. **"Output Data"** means generated outputs such as predictions, information, content, recommendations, or decisions provided by an AI System in response to processing Input Data.

z. "**Personally Identifiable Information**" means personal data or information that relates to a specific, identifiable, individual person, including County personnel, and includes all variations of that term as defined in the Applicable Data and Security Privacy Laws. For the avoidance of doubt, Personally Identifiable Information includes: (a) any government-issued identification numbers (e.g.,

Social Security, driver's license, passport); (b) any financial account information, including account numbers, credit card numbers, debit card numbers, and other Cardholder Data; (c) Criminal Justice Information; (d) Protected Health Information; (e) Biometric Information; (f) passwords or other access-related information associated with any user account; and (g) any other personal data defined as Personally Identifiable Information under Data Breach Notification Laws.

aa. **"Personal Health Information"** means information relating to the past, present, or future physical or mental health or condition of an individual; to the provision of health care to an individual; or to payment (whether past, present, or future) for health care ; and either (i) Identifies the individual; or (ii) provides sufficient information that could reasonably be used to identify the individual, but that is not included in the definition of Protected Health Information under 45 C.F.R. 160.103.

bb. "**Protected Health Information**" or "**PHI**" has the same meaning as the term "Protected Health Information" in 45 C.F.R. 160.103.

cc. "**Services**" means the same meaning as defined in Article 3 of the County Professional Services Agreement or "Deliverables" as defined in the County Instruction to Bidders and General Conditions, if either document forms the basis of this Agreement.

dd. "**Software**" means computer programs, whether in source code or object code form (including any and all software implementation of algorithms, models and methodologies), databases and compilations (including any and all data and collections of data), and all documentation (including user manuals and training materials) related to the foregoing.

ee. "**Third-Party Vendor**" means any subcontractor, company, independent contractor, or vendor of any kind that is not a direct employee or corporate division of Consultant. Third Party Vendors includes Subconsultants as may be defined in the Underlying Contract.

II. Data Storage and Access

a. **Data Storage**: Consultant agrees to store all County Data in compliance with Section III Privacy and Data Security of this document. Consultant agrees to ensure that County Data it receives and stores is kept in the same technical format (not including the application of encryption) and is organized in the same manner (as close to a 1 to 1 storage as possible) as it was received by Consultant.

Consultant also agrees to minimize storing or transferring County Data on portable media devices and will only store or transfer County Data on portable media devices with prior written approval from County. Should it be necessary to store or

transfer County Data via a portable media device, Consultant agrees to secure the same with commercially available cybersecurity tools (i.e., requiring multi-factor authentication to access such portable media device), and to track in a security log all instances of downloads of County Data to a portable media device and the chain of custody of such media device until County Data is securely deleted from same. Consultant further agrees that any such portable media device will fully encrypt the data, and that authority to access or remove the portable media device containing County Data is granted only with demonstrated need. Consultant will only utilize portable media devices with the ability to be remotely wiped

b. **Approved Facilities:** Consultant will perform Services and host County Data only within the continental United States and only from locations owned or leased by Consultant and its Subcontractors.

c. **Data Minimization:** Consultant must implement procedures to minimize collection of Personally Identifiable Information and Personal Health Information. If Personally Identifiable Information must be collected or processed by Consultant on County's behalf, or is shared with Consultant by County for any reason, Consultant will only use such Personally Identifiable Information: (i) as directed by the County; (ii) as needed to provide contracted services to the County; and (iii) for no other purpose. If Personally Identifiable Information must be shared with a third party, Consultant will only share portions of such information necessary to accomplish the purpose of sharing and that it will comply with all requirements of Section V before sharing with such third party.

d. **Data Access and E-Discovery**: The County may access and copy any County Data in Consultant's possession at any time for any reason, without limitation. Consultant shall reasonably facilitate such access and copying promptly after the County's request.

   Consultant agrees to only delete County Data in compliance with applicable law and the Data Deletion section of this Agreement. Consultant also agrees to halt any deletion of County Data promptly, including directing its Third-Party Vendors to do the same, if the County informs Consultant in writing that such data must be preserved.

e. **Compliance with Applicable Data Applicable Data Security and Privacy Law(s)**: If the County is required to respond to a Data Subject Request, Consultant agrees to reasonably cooperate with the County to the full extent necessary to respond in compliance with Applicable Data Security and Privacy Laws. If Consultant receives a Data Subject Request related to this Agreement, Consultant will notify County of such request as soon as reasonably practicable and will reasonably cooperate with the County to the full extent necessary to respond in compliance with Applicable Data Security and Privacy Laws.

f. **County Confidential Information**. All County Confidential Information shall remain the property of the County, and no license or other rights to the Consultant is granted or implied hereby. Consultant shall not disclose or allow disclosure of any of the County's Confidential Information to any third party, except to Consultant's employees and representatives, who are subject to written and enforced obligations to keep such Confidential Information confidential, and shall only use and disclose such County Confidential Information (i) for purposes of performing its obligations under this Agreement, and/or (ii) in connection with any SOW/Order Form (including in the course of discussions or exploration of a potential SOW/Order Form which may or may not ultimately be executed). Consultant remains responsible for any breach of this section by its employees and representatives.

   i. In the event that Consultant is required to disclose County Confidential Information in accordance with a judicial or governmental requirement or order, Consultant shall limit disclosure of such data in compliance with Section III(c)(iii) of this Addendum.

   ii. County Confidential Information shall be subject to the confidentiality obligations of this Section III(f) for ten years following Consultant's return or destruction of County Confidential Information in accordance with subsection iv below.

   iii. **Injunctive Relief**. Consultant acknowledges that disclosure of any County Confidential Information by it or its employees or representatives may give rise to irreparable injury to the County not adequately compensated by damages. Accordingly, the County may be entitled to equitable relief, including injunctive relief and specific performance against the breach or threatened breach of the undertakings in this section, in addition to any other legal remedies that may be available.

   iv. **Return or Destruction of County Confidential Information**. Unless otherwise provided in this Agreement, upon the earlier of the County's request or termination or expiration of this Agreement, Consultant shall, at the County's option, promptly destroy or return all County Confidential Information, including all copies in any form or medium, in its possession or control, in compliance with Section III(e) of this Addendum.

g. **Information Access**: Consultant may not permit access to any County Confidential Information by any unauthorized individual or entity. Consultant must provide its personnel only such access as is minimally necessary for such persons/entities to perform the tasks and functions for which they are responsible. Consultant will, upon request from the County, provide the County with an updated list of its personnel with access to County Data and the level of such access.

h. **Public Records Laws**: Consultant will comply with all laws governing public records located at 50 ILCS 205/1 et seq. and at 44 Ill. Admin. Code 4500.10 et seq.

Specifically, and without limitation, Consultant must: (a) store County Data such that each record is individually accessible for the length of the County's scheduled retention; (b) retain a minimum of two copies of all County Data according to industry best practices for geographic redundancy, such as NIST Special Publication 800-34 as revised; (c) store and access County Data in a manner allowing individual records to maintain their relationships with one another; (d) capture relevant structural, descriptive, and administrative metadata to County Data at the time a record is created or enters the control of Consultant.

III. Privacy and Data Security

a. **General Requirement of Confidentiality and Security**: Consultant will maintain the confidentiality and security of all County Data that it has copies of or access to. Without limiting Consultant's other obligations under this Agreement, Consultant must use commercially available and state-of-the-art cybersecurity tools and controls meeting this Section III's requirements to provide reasonably appropriate security protection to County Data proportionate to the type and sensitivity of County Data at issue. Similarly, Consultant must provide and perform all Services and Software securely in compliance with the requirements of this Section III using security technologies and techniques in accordance with industry-leading practices and County security policies, procedures and other requirements made available to Consultant in writing. This includes network management and maintenance applications and tools, appropriate fraud prevention and detection and encryption technologies to protect County Confidential Information. Consultant must secure all Personally Identifiable Information with the highest level security commercially available, and must also encrypt all Personally Identifiable Information and Personal Health Information in transit, and at rest. The requirements of this Section III shall apply to all of Consultant's Systems and the facilities where such Consultant Systems are used to collect, store, handle, process, backup, dispose, and/or access County Data.

b. **Applicable Data Security and Privacy Laws:** Consultant agrees to comply with and abide by all Applicable Data Security and Privacy Laws, including those applicable to the Consultant if it, rather than the County, were the owner or data controller of any County Data in its possession or under its control in connection with the Services.

c. **Data Ownership:** Consultant recognizes and agrees that the County possesses and retains all right, title, and interest in and to County Data, and that Consultant's use, access to and possession thereof is solely to fulfill its obligations under this Agreement and that any processing and use of County Data by the Consultant is done solely on the County's behalf and for the County's benefit.

i. Consultant further recognizes and agrees that:
    1. County Data is valuable property of the County and may include proprietary, sensitive, private and/or trade secret information; and
    2. County Data may include original compilation pursuant to copyright laws of the United States and other jurisdictions; and
    3. The County has dedicated substantial resources to collecting, managing, securing and compiling County Data; and
    4. County may suffer irreparable harm or loss in the event of such information being disclosed or used otherwise than in accordance with this Agreement; and
    5. Without the County's express written consent, no County Data, or any part thereof, may be disclosed, assigned, destroyed, altered, withheld, or otherwise restricted by Consultant or commercially exploited by or on behalf of Consultant.

ii. The County grants Consultant a limited, non-transferrable and royalty free license to use and access County Data solely as necessary to fulfill Consultant's duties under this Agreement. Without County's prior written consent, Consultant shall not:
    1. access or use any County Data for any purpose other than to fulfill its duties and obligations under this Agreement; or
    2. give third party access to or copies of County Data, unless in compliance with the Third-Party Vendor section below.

iii. In the event that Consultant is required to disclose County Data in accordance with a judicial or governmental requirement or order, Consultant will, except to the extent prohibited by law:
    1. give the County reasonable prior notice and opportunity to object or seek a protective order or other appropriate remedy;
    2. Cooperate with the County so the County may object to or seek a protective order or other appropriate remedy;
    3. disclose only portion(s) of the County Data that it is legally required to disclose.

d.

e. **Consultant as a Data Processor**: Consultant understands and acknowledges that, to the extent that performance of its obligations hereunder involves or necessitates processing Personally Identifiable Information, it will act only on direction from the County.

f. **Data Deletion**: Consultant agrees that at the conclusion of this Agreement or upon the written request of the County, it will promptly:
    i. Make available for retrieval all versions and copies of County Data to the County in such a format that the County may reasonably request and;
        1. provide County with adequate bandwidth and other resources to remove County Data from Consultant servers; and

2. provide sufficient information requested by the County about the format and structure of the County Data to enable such data to be used in substantially the same manner as used by Consultant.

ii. Axon will not delete Customer Content for one hundred eighty (180) days following termination. Axon Cloud Services will not be functional during these one hundred eighty (180) days other than the ability to retrieve Customer Content. Axon has no obligation to maintain or provide Customer Content after these one hundred eighty (180) 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.

iii. direct and ensure secure erasure of County Data by any and all of Consultant's Third-Party Vendors with copies of or access to County Data.

Consultant also agrees that in deleting County Data as required by this Agreement, Consultant shall leave no data readable, decipherable, or recoverable on its computers, servers, or other media, or those of its Third-Party Vendors, in accordance with NIST Special Publication 800-88 as revised. Promptly after Consultant has completed its deletion of County Data and has directed its Third-Party Vendors to do the same, and no later than 180 days after termination of this Agreement. Upon written request, Consultant shall certify such deletion to County in writing in compliance with NIST Special Publication 800-88.

g. **Data Security:** Without limiting any of its other obligations and promises elsewhere in the Agreement, Consultant shall prevent unauthorized access to, sharing, disclosure, modification, or destruction of County Data. Consultant represents and warrants that:

i. it will not permit any unauthorized access to or allow its actions or inactions to cause any loss or damage to County Data or County IP;

ii. it will comply with any and all County security policies in place during the term of this Agreement;

iii. it will not use any system that is dependent on software or hardware without appropriate security updates available;

iv. it will only store County data within the Continental United States;

v. it will appropriately vet using, at a minimum, criminal background checks, identity verification of physical person to a government issued id card, and employment history verification of all employees and representatives working with or provided access to County Data and County IP and ensure that such employees and representatives are legally bound to maintain the security and confidence of County Data, County IP, and County Confidential Information; and

vi. it will not allow any foreign government or foreign owned organizations or other third parties access to any County Data, County IP, or County Confidential Information.

h. **Information Security Program**: Consultant agrees to maintain, implement, and comply with a written Information Security Program requiring industry standard administrative, technical, and physical safeguards appropriate to:
   i. protect the security and confidentiality of County Data;
   ii. identify and protect against threats and hazards to the security or integrity of County Data; and
   iii. protect against unauthorized access, taking, sharing, destruction, modification, or use of County Data.

   Consultant's administrative, technical, and physical safeguards must provide a level and scope of security not less than the level and scope required under (a) the County Policies as updated; (b) Federal Information Processing Standard 200; (c) then-current NIST 800-series standard and successors thereto; or (d) an equivalent, generally accepted, industry-standard and state-of-the-art security standards series.

   Consultant shall also ensure that the Information Security Program addresses the following:
   i. Proper disposal of County Data once it is no longer needed to carry out the purposes of this Agreement and in compliance with the Data Deletion section of this Agreement;
   ii. Access controls on systems and servers used to maintain, access, or transmit County Data;
   iii. Access restrictions and appropriate security controls at physical locations containing County Data, including at servers and/or data banks;
   iv. Multi-Factor Authentication on all systems, accounts, and endpoints, with access to store or maintain County Data;
   v. Encryption of electronic County Data, at rest and in transit, in a manner that, at a minimum, adheres to NIST SP 800-111, NIST SP 800-52, NIST SP 800-77 and NIST SP 800-113 encryption standards, and maintain current version of these standards.
   vi. Application of least privilege principles for access to County Data, which is supplemented either by dual control procedures or segregation of duties;
   vii. Regular testing and monitoring of electronic systems accessing or storing County Data; and
   viii. Procedures to detect actual and attempted attacks on or intrusions into the end points, systems, or servers, containing or accessing County Data.

i. **Regular Review of Security Program**: Consultant shall review the Information Security Program regularly, but no less than annually, and update them to comply with applicable laws, regulations, technology changes, and best practices.

j. **Cyber Incident**: Consultant represents and warrants that it maintains the cybersecurity of its Services and Software and takes proactive and consistent action and to prevent a Cyber Incident from affecting any County IT environment at any time. If Consultant discovers that a Cyber Incident has impacted its own environment and has or has the potential to impact the County's IT environment, Consultant must, at no additional charge, (a) immediately undertake to address the Cyber Incident to mitigate damage and restore any affected Service, Software or equipment; (b) notify the County in writing within 48 hours of discovery of the incident; and (c) use reasonable efforts to correct and repair any damage to County Data or Software and otherwise assist the County in mitigating such damage and restoring any affected Service, Software or equipment.

k. **Data Breach**: In the event that Consultant suffers a Data Breach of County Data, it agrees to:
   I. Notify County promptly and without unreasonably delay, but no later than 48 hours after discovery of the Data Breach. Notification shall be sent to administrators registered on Axon Cloud Services;
   II. Notify County promptly and without unreasonable delay, but no later than 48 hours after receiving notification from a Third-Party Vendor, of a Data Breach suffered by such vendor, if Consultant confirms Data Breach affects County Data. Notification shall be sent to administrators registered on Axon Cloud Services;
   III. If the Data Breach concerns County Data:
      1. Consultant will reasonably provide County with meaningful information of the forensic investigation, including details regarding method of compromise, identity of the attackers if known and progress of remediation;
      2. Consultant will assist the County as it seeks to comply with any data breach notification requirements. Such assistance shall include not be limited to, providing the County with access to data, personnel and information relating to the County Data that may have been exposed, and, if applicable, information about any persons whose Personally Identifiable Information may have been affected or exposed;
      3. Consultant will notify any affected persons solely at the County's direction, including review and approval of all notices, and governmental regulators, as applicable;
      4. Consultant will recover affected data or information to the extent possible;
      5. Consultant will provide County with a corrective action plan mutually acceptable to County;
      6. Consultant will not make any public announcements relating to such Data Breach without the County's prior written approval; and

7. Consultant agrees that County has the sole right to (a) determine whether notice of any Data Breach involving County Data is to be provided and to whom; and (b) approve the contents of such notice, whether any type of remediation may be offered to affected persons, and the nature and extent of any such remediation.

IV. In the event of a Data Breach attributable to an act or omission of Contractor, including without limitation those of Consultant's Third-Party Vendors, subcontractors or other agents, except to the extent any Data Breach is caused by the acts or omissions of the County, Consultant shall also:
    1. reimburse County for any and all reasonable expenses related to data breach notifications, including the provision of credit monitoring services to affected persons;
    2. indemnify and defend the County from any and all legal actions that arise from such data breach; and
    3. compensate the County for any and all other related costs or expenses, such as recreating lost or compromised data.

V. Nothing in this section is meant to limit or restrict any of the County's other rights or potential remedies stemming from such data breach.

l. **Data Integrity and Loss of County Confidential Information.** Consultant must implement and maintain strong, industry standard measures, as detailed in Section III(g) of this Addendum, to maintain accuracy of County Data. Without limiting any rights and responsibilities under this Section III in the event of any disclosure, inaccuracy, or loss of, or inability to account for, any County Confidential Information, Consultant must promptly, at its own expense: (a) notify the County in writing within 48 hours; (b) take such actions as necessary or reasonably requested by the County to minimize the violation; and (c) cooperate in all reasonable respects with the County to minimize any damage resulting from the violation.

m. **Biometric Data Security and Breach**: If Consultant will receive, handle, manage, store, review, collect, access, or otherwise process any Biometric Information as a part of this Agreement:
    i. Consultant will provide its written policies related to the retention schedule and permanent deletion of Biometric Information to County prior to Consultant's receipt of the Biometric Information.
    ii. If this Agreement requires Consultant to collect Biometric Information on behalf of the County, Consultant agrees to obtain appropriate consent, as required by the Illinois Biometric Information Privacy Act (740 ILCS 14/1, et seq.), from the person who the Biometric Information is being collected from, on behalf of both Consultant and the County.

iii. Consultant agrees that under no circumstances will it sell, lease, trade, or otherwise profit from Biometric Information in connection with this Agreement, regardless of whether received from the County or collected directly from the person.

iv. Consultant shall ensure that its Information Security Program, as required via this Section III, provides for and includes protection of Biometric Information. Additionally, Consultant agrees to implement any additional data security policies and controls for Biometric Information as necessary to ensure full compliance with applicable privacy laws.

Consultant shall notify County promptly and without unreasonably delay, but no later than 48 hours after discovery, of any Data Breach affecting Biometric Information. Notification shall be sent to administrators registered on Axon Cloud Services.

n. **Payment Card Data Security and Breach**: **Intentionally omitted.**

o. **PHI Data Security and Breach**: If the Underlying Contract requires or permits Consultant to receive, handle, manage, store, review, collect, access, or otherwise process any PHI, then Consultant agrees:

i. that in addition to this Agreement, it must enter into a Business Associate Agreement with the County entity or division providing Consultant with copies of or access to the PHI.

ii. that its Information Security Program, as required via this Section III, provides for and includes the protection of PHI. Additionally, to the extent necessary, Consultant agrees to implement any additional data security policies and controls for PHI to ensure full compliance with both the Health Insurance Portability and Accountability Act of 1996 (Pub. L. 104-191, 110 Stat. 1936, 45 CFR 160, et. seq.) and the Health Information Technology for Economic and Clinical Health Act (Pub. L. No. 111-5, Title XIII, 123 Stat 226).

iii. to notify the County promptly and without unreasonably delay, but no later than 48 hours after discovery, of any Data Breach affecting PHI. Notification shall be sent to administrators registered on Axon Cloud Services.

p. **CJIS Data Security and Breach**: If the Underlying Contract requires or permits that Consultant receive, handle, manage, store, review, collect, access, or otherwise process any CJIS Information, then Consultant agrees:

i. to sign and return to the County, in paper or electronic copy, the CJIS Data Security Acknowledgement Receipt after the County provides Consultant with a copy of this Addendum and the CJIS Security Policy.

ii. that its Information Security Program, as required via Section III(f) of this Addendum, provides for and includes the protection of CJIS Information. Additionally, to the extent necessary, Consultant agrees to implement any

additional data security policies and controls for CJIS Information to ensure full compliance with both the Criminal Justice Information Services Security Policy and the policies and standards established by the Criminal Justice Information Services Advisory Policy Board.

iii. to sign and abide by an Information Exchange Agreement with the County prior to any exchange of CJIS Information.

iv. Notify County promptly and without unreasonable delay, but no later than 48 hours after discovery, of any Data Breach affecting CJIS Information. Notification shall be sent to administrators registered on Axon Cloud Services.

q. **Privacy Notice**: Consultant shall provide effective notice to the public and to individuals regarding:

i. Its activities that impact privacy, including its collection, use, sharing, safeguarding, maintenance, and disposal of personally identifiable information (PII); and

1. Authority for collecting PII; and
2. The choices, if any, individuals may have regarding how Consultant uses PII and the consequences of exercising or not exercising those choices; and
3. The ability to access and have PII amended or corrected if necessary.

ii. The Consultant's privacy notice shall describe:

1. The PII collected and the purpose(s) for which it collects that information; and
2. How the Consultant uses PII internally; and
3. Whether individuals have the ability to consent to specific uses or sharing of PII and how to exercise any such consent; and
4. How individuals may obtain access to their PII; and how PII will be protected.

IV. **Consultant Personnel**: Consultant will oblige its personnel to comply with applicable Data Protection Laws and to undertake only to collect, process or use County Data necessary to perform the Services, and will not make it available to any Third Parties except as specifically authorized hereunder. Consultant must ensure that, prior to performing any Services or accessing any County Data or other County Confidential Information, all Consultant personnel who may have access to the aforementioned must execute agreements concerning access protection and data/software security consistent with this Agreement.

V. **Third-Party Vendors:** Consultant agrees that if it is to utilize third party vendors for this Agreement that require access to or copies of County Data in order to perform its work, that it will:

a. Ensure that all such vendors and their employees are located within the Continental United States, unless approved in writing in advance by County;

b. Ensure that no such vendor is owned in part or in whole by a foreign government, unless approved in writing in advance by County;
c. Provide a written list of such vendors to the County, along with a link to or copy of the vendors' privacy and data security policy;
d. Ensure that Consultant's contracts with such vendors contain the appropriate data security and privacy protections for County Data that are the same or at least as stringent as the provisions contained within this Agreement;
e. Ensure that each vendor is required to promptly notify Consultant of any Data Breach suffered by the vendor that concerns County Data;
f. Notify County within 48 hours upon receiving notification from a vendor of any Data Breach that concerns County Data;
g. Remain responsible for any resulting costs, liability, charges or expenses incurred by the County and stemming from the action or inaction of such Third-Party Vendor; and
h. In the event of a Data Breach stemming from such vendor, assist the County with obtaining information, documents, and access to persons necessary to investigate such Data Breach and provide necessary legal notifications.

Customer has determined and approve the following subprocessors and processing locations by designating one of the following economic area:

Name of entity	**Address of entity**	**Location of provision of the Services**	**Description of Services and Purpose**	**External Links with More Information**
Microsoft Corporation *(ONLY Azure Services)*	One Microsoft Way, Redmond, WA 98052	United States	Microsoft Azure Services provide infrastructure and platform services, which include providing cloud storage for Customer Content.	Microsoft Privacy Statement
Amazon Web Services Inc.	410 Terry Avenue North, Seattle, WA	United States	AWS provides infrastructure and platform services, which include providing cloud storage for Customer Content.	AWS Privacy Notice

	98109-5210			
Twilio Inc	101 Spear Street, Fifth Floor, San Francisco, California, 94105, United States	United States	Messaging and SMS provider	Twilio Privacy Notice

VI. Audit Rights

a. **Data Security Audit**: Consultant agrees to have a Security Audit Service Organization Control (SOC 2), Type II Audit performed at least annually, and, at its sole cost and expense, to provide the County and its auditors with the SOC 2, Type II report, or its equivalent, for all locations at which the County Data is processed or stored.

Further, Consultant agrees that it will promptly make available within 30 days upon written request from the County the executive summary of any reviews or audits (other than the annual SOC 2 audit) conducted by Consultant (including Consultant's internal and external auditors).

b. **Third Party Vendor Audits**: **Intentionally Omitted**

c. **CJIS Information Audits:** To the extent that this Agreement concerns CJIS Information, Consultant agrees that, in addition to the County's audit rights, the FBI may also be authorized to perform a security audit of Consultant's and/or Consultant's vendor's systems during the pendency of this Agreement and a final audit at the termination of this Agreement.

VII. Intellectual Property

a. **Consultant Intellectual Property Warranty**: Consultant represents and warrants that it owns, or is authorized to use, all Consultant IP, and Consultant-provided third-party IP.

b. **Open Source Material**: Consultant represents and warrants that all open source materials (OSM) included in Deliverables or Software are obtained from a trusted distributor. Consultant represents and warrants that all OSM materials provided to County or used on County's behalf comply with their license agreements. Unless otherwise specified in this Agreement, Consultant must maintain OSM support, including required patching and security updates, which will be provided promptly after release. Consultant must not use any materials allowing users to modify or incorporate open source code into larger programs on the condition that the software containing the source code is publicly distributed without restrictions, commonly known as "copyleft."
c. **Developed Intellectual Property**: To the extent that any Intellectual Property specifically developed solely and exclusively for the County by Consultant under the terms of this Agreement, Consultant hereby irrevocably and unconditionally assigns, transfers, and conveys to the County, without further consideration, all of its right, title, and interest in such Developed Intellectual Property. This transfer will take place immediately upon the creation and completion of such works without need for further documentation or action on the part of the Parties. Consultant agrees to perform any actions as may reasonably be necessary, or as the County may reasonably request, to perfect the County's ownership of any such Developed Intellectual Property.
d. **Software Licenses**: This Agreement contains all terms and conditions relating to any and all licenses in Consultant-Provided Software and Consultant Intellectual Property. Except as explicitly set forth elsewhere in this Agreement, all licenses that Consultant grants in Consultant-Provided Software include: (a) the right of use by Third Party Consultant for the benefit of the County, (b) the right to make backup copies, and (c) the right to reasonably approve the procedures by which Consultant may audit the use of license entitlements.
e. **County Intellectual Property**: Consultant acknowledges that County retains all right, title and interest in and to all County IP. Consultant will not be permitted to use any County IP for the benefit of any entities other than the County. Upon expiration or termination of this Agreement, Consultant must cease all use of County IP and must return to the County all County IP.
f. **Residual Knowledge**: Consultant acknowledges that nothing contained in this Agreement restricts either Party from the use of ideas, concepts, know-how, or techniques relating to the Services which either Party, individually or jointly, develops or discloses under this Agreement, provided that in doing so (a) such information is solely retained in the unaided memory of the Parties' employees performing or using such Services, (b) the Party does not breach its respective obligations under Section III relating to confidentiality and non-disclosure, and (c) such use does not infringe the Intellectual Property rights of other parties who have licensed or provided materials to the other. Except for the license rights contained in this Section VII, neither this Agreement nor any disclosure made hereunder grants any license to either Party under any Intellectual Property rights of the other.

g. **Export Laws**: Consultant will comply with all laws governing the export of intellectual property, including the Export Administration Regulations, 15 CFR 730, et seq.

VIII. Other Provisions

a. **Processing by an AI System:** To the extent that the Software and/or Services allow for County Data to be processed by an AI System, any Input Data that is entered into the AI System by County will be considered County Data, and County will have the same right to use and display any Output Data that has been generated in response to the Input Data entered into the AI System by the County. Consultant remains the owner of all Evolution Data, but only to the extent that it can establish that the Evolution Data does not contain any Personally Identifiable Information or County Confidential Information.

b. **Accessibility Requirements under the Americans with Disabilities Act**: If this contract includes information technology systems that are required by federal law to be "accessible," consultant must sign an Americans with Disabilities Act (ADA) Accessibility Addendum. See Americans with Disabilities Act – Cook County Accessibility Requirements Exhibit, attached hereto and incorporated by this reference, which further describes Consultant's accessibility obligations and must be submitted to the County to reflect compliance. Except as specifically set forth in Exhibit XXX, Consultant acknowledges the County is relying upon Contractor to ensure compliance with Title II of the Americans with Disabilities Act (ADA), its implementing regulations adopted by the federal government, and the accessibility standards set forth in the Web Content Accessibility Guidelines (WCAG) 2.1, level AA published by the World Wide Web Consortium (W3C).

c. **Removal of Consultant Materials**: Consultant is responsible, at its own expense, for de-installation and removal of any equipment, software, or hardware, owned, licensed, or leased by Consultant, and provided to the County, to facilitate the provision of Services under this Agreement, and that is not being transferred to the County under the Agreement. Consultant shall comply with all reasonable County requests and procedures related to the deinstallation and removal , and agrees to do so in a manner that minimizes adverse impact or working disruptions to the County or its employees.

d. **Resources Necessary for Services**. Except as set forth in this Agreement, Consultant will provide and is financially responsible for all equipment, Software, and other resources needed to perform the Services in accordance with the Agreement. Consultant agrees that it keep all required equipment, Software, and other resources functional.

e. **Required Consents for Assets in Use and Third-Party Contracts as of the Effective Date**. For this section, "Assets" mean equipment, Software, Intellectual Property and other assets used in providing the Services and "Required Consent" means the consent required to secure any rights of use of or access to any of County-provided or third-party Assets that are required by Consultant to perform the Services. Consultant is responsible for obtaining all Required Consents relating to

this Agreement. The County will cooperate with Consultant and provide Consultant such assistance in this regard as the Consultant may reasonably request.

f. **Updates**. Consultant must provide to the County, without charge, the timely application of any upgrades to software required for Services that are available free of charge to third parties. Software upgrades must include, but not be limited to, new version releases and operating system patching, as well as bug fixes and other security-related updates.

g. **No Click-Wrap or Incorporated Terms.** The County is not bound by any content on Consultant's website, including any click-wrap, cookies consents, or other similar document.

h. **Resale of Equipment and Software**. If Consultant resells to the County any equipment or Software that Consultant purchases from a Third Party, Consultant, to the extent it is legally able to do so, must pass through any such third-party warranties to the County and reasonably cooperate in enforcing them. Such warranty pass-through will not relieve Consultant from its warranty obligations set forth in this Agreement.

i. **Warranty for Developed Software**: Consultant represents and warrants that all developed software solely and exclusively for the County will be free from material errors in operation and will comply with the applicable documentation and specifications in all material respects for twelve (12) months after the installation, testing, and acceptance of such developed software by the County. Any repairs to developed software pursuant to this Section will receive a new twelve (12) month warranty period.

IX. **Indemnity**: In addition to and not in derogation of any indemnification provisions in the Professional Service Agreement, Consultant shall defend, hold harmless, and indemnify the County against any third party claim, suit, or proceeding arising out of a Data Breach. or Consultant's violation of any Privacy or Data Security law, including without limitation any breaches or violations committed by or through Consultant's agents, employees, representatives, licensees, invitees, or Third-Party Vendors, except to the extent any such Data Breach or violation is caused by the acts or omissions of the County, its employees, agents, or contractors.

X. **Limitation of Liability Exceptions**: Any limitation of liability contained in the Underlying Contract does not apply to:

a. any breach of the Privacy and Data security section of this Agreement;
b. any Data Breach concerning County Data and stemming from Consultant or its Third Party Vendor(s);
c. any breach of the Third-Party Vendor section of this Agreement; or
d. losses caused by the gross negligence or willful misconduct of Consultant.

XI. **Enforceability**: If any provision of this Agreement is deemed invalid or unenforceable, the Agreement will be amended to the minimum extent necessary to achieve, to the maximum extent possible, the same legal and commercial effect originally intended by the parties. To

the extent permitted by applicable law, the parties waive any provision of law that would render any clause of this Agreement prohibited or unenforceable in any respect.

XII. **Survival**: This Data Security and Privacy Addendum shall survive for a period of ten (10) years from either (i) the expiration or termination of the Agreement, or (ii) the return and certified secure destruction of County Data.

XIII. **No Limitation**. The rights and obligations set forth in these IT and Data Special Conditions exhibit do not limit the rights and obligations set forth in any Articles of the Professional Services Agreement.

EXHIBIT 5

CJIS Security Addendum

APPENDIX H SECURITY ADDENDUM

The following pages contain the legal authority, purpose, and genesis of the Criminal Justice Information Services Security Addendum (H2-H4); the Security Addendum itself (H5-H6); and the Security Addendum Certification page (H7).

FEDERAL BUREAU OF INVESTIGATION
CRIMINAL JUSTICE INFORMATION SERVICES
SECURITY ADDENDUM

Legal Authority for and Purpose and Genesis of the Security Addendum

Traditionally, law enforcement and other criminal justice agencies have been responsible for the confidentiality of their information. Accordingly, until mid-1999, the Code of Federal Regulations Title 28, Part 20, subpart C, and the National Crime Information Center (NCIC) policy paper approved December 6, 1982, required that the management and exchange of criminal justice information be performed by a criminal justice agency or, in certain circumstances, by a noncriminal justice agency under the management control of a criminal justice agency.

In light of the increasing desire of governmental agencies to contract with private entities to perform administration of criminal justice functions, the FBI sought and obtained approval from the United States Department of Justice (DOJ) to permit such privatization of traditional law enforcement functions under certain controlled circumstances. In the Federal Register of May 10, 1999, the FBI published a Notice of Proposed Rulemaking, announcing as follows:

> 1. Access to CHRI [Criminal History Record Information] and Related Information, Subject to Appropriate Controls, by a Private Contractor Pursuant to a Specific Agreement with an Authorized Governmental Agency To Perform an Administration of Criminal Justice Function (Privatization). Section 534 of title 28 of the United States Code authorizes the Attorney General to exchange identification, criminal identification, crime, and other records for the official use of authorized officials of the federal government, the states, cities, and penal and other institutions. This statute also provides, however, that such exchanges are subject to cancellation if dissemination is made outside the receiving departments or related agencies. Agencies authorized access to CHRI traditionally have been hesitant to disclose that information, even in furtherance of authorized criminal justice functions, to anyone other than actual agency employees lest such disclosure be viewed as unauthorized. In recent years, however, governmental agencies seeking greater efficiency and economy have become increasingly interested in obtaining support services for the administration of criminal justice from the private sector. With the concurrence of the FBI's Criminal Justice Information Services (CJIS) Advisory Policy Board, the DOJ has concluded that disclosures to private persons and entities providing support services for criminal justice agencies may, when subject to appropriate controls, properly be viewed as permissible disclosures for purposes of compliance with 28 U.S.C. 534.
>
> We are therefore proposing to revise 28 CFR 20.33(a)(7) to provide express authority for such arrangements. The proposed authority is similar to the authority that already exists in 28 CFR 20.21(b)(3) for state and local CHRI systems. Provision of CHRI under this authority would only be permitted pursuant to a specific agreement with an authorized governmental agency for the purpose of providing services for the administration of criminal justice. The agreement would be required to incorporate a security addendum approved by the Director of the FBI (acting for the Attorney General). The security

addendum would specifically authorize access to CHRI, limit the use of the information to the specific purposes for which it is being provided, ensure the security and confidentiality of the information consistent with applicable laws and regulations, provide for sanctions, and contain such other provisions as the Director of the FBI (acting for the Attorney General) may require. The security addendum, buttressed by ongoing audit programs of both the FBI and the sponsoring governmental agency, will provide an appropriate balance between the benefits of privatization, protection of individual privacy interests, and preservation of the security of the FBI's CHRI systems.

The FBI will develop a security addendum to be made available to interested governmental agencies. We anticipate that the security addendum will include physical and personnel security constraints historically required by NCIC security practices and other programmatic requirements, together with personal integrity and electronic security provisions comparable to those in NCIC User Agreements between the FBI and criminal justice agencies, and in existing Management Control Agreements between criminal justice agencies and noncriminal justice governmental entities. The security addendum will make clear that access to CHRI will be limited to those officers and employees of the private contractor or its subcontractor who require the information to properly perform services for the sponsoring governmental agency, and that the service provider may not access, modify, use, or disseminate such information for inconsistent or unauthorized purposes.

Consistent with such intent, Title 28 of the Code of Federal Regulations (C.F.R.) was amended to read:

§ 20.33 Dissemination of criminal history record information.

a) Criminal history record information contained in the Interstate Identification Index (III) System and the Fingerprint Identification Records System (FIRS) may be made available:

1) To criminal justice agencies for criminal justice purposes, which purposes include the screening of employees or applicants for employment hired by criminal justice agencies.

2) To noncriminal justice governmental agencies performing criminal justice dispatching functions or data processing/information services for criminal justice agencies; and

3) To private contractors pursuant to a specific agreement with an agency identified in paragraphs (a)(1) or (a)(6) of this section and for the purpose of providing services for the administration of criminal justice pursuant to that agreement. The agreement must incorporate a security addendum approved by the Attorney General of the United States, which shall specifically authorize access to criminal history record information, limit the use of the information to the purposes for which it is provided, ensure the security and confidentiality of the information consistent with these regulations, provide for sanctions, and contain such other provisions as the Attorney General may require. The power

and authority of the Attorney General hereunder shall be exercised by the FBI Director (or the Director's designee).

This Security Addendum, appended to and incorporated by reference in a government-private sector contract entered into for such purpose, is intended to insure that the benefits of privatization are not attained with any accompanying degradation in the security of the national system of criminal records accessed by the contracting private party. This Security Addendum addresses both concerns for personal integrity and electronic security which have been addressed in previously executed user agreements and management control agreements.

A government agency may privatize functions traditionally performed by criminal justice agencies (or noncriminal justice agencies acting under a management control agreement), subject to the terms of this Security Addendum. If privatized, access by a private contractor's personnel to NCIC data and other CJIS information is restricted to only that necessary to perform the privatized tasks consistent with the government agency's function and the focus of the contract. If privatized the contractor may not access, modify, use or disseminate such data in any manner not expressly authorized by the government agency in consultation with the FBI.

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.

_____ _____

Printed Name/Signature of Contractor Employee Date

_____ _____

Printed Name/Signature of Contractor Representative Date

_____

Organization and Title of Contractor Representative

FEDERAL BUREAU OF INVESTIGATION
CRIMINAL JUSTICE INFORMATION SERVICES
SECURITY ADDENDUM

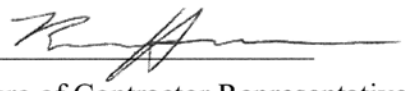
CERTIFICATION

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.

_____ _____

Printed Name/Signature of Contractor Employee Date

Benjamin Hagen  _____

Printed Name/Signature of Contractor Representative Date

Axon Enterprise, Inc. / CISO

Organization and Title of Contractor Representative

EXHIBIT 6

Minority and Women Owned Business Enterprise Commitment

COOK COUNTY
OFFICE OF THE
Chief Procurement
Officer

161 N. Clark
Suite 2300
Chicago, Illinois 60601

Memorandum

Date: December 04, 2025

TO: Raffi Sarrafian, Chief Procurement Officer
Office of the Chief Procurement Officer

FROM: JEANETTA CARDINE
Jeanetta Cardine, Deputy Director
Compliance Center of Excellence
Center of Business Enterprise Development

RE: Contract Number: 2526-10211
Digital Evidence Management System
States Attorneys Office
Contractor: Axon Enterprises, Inc.
Award Amount: $11,101,643.12
Anticipated Contract Term: January 01, 2026 - December 31, 2030 Piggyback – Professional Services
Participation Goal: 0% MBE & 0% WBE

Dear Mr. Sarrafian:

The Center of Business Enterprise Development is in receipt of the above-piggyback solicitation and has determined a 0% MBE & 0% WWBE participation goal was recommended and does not require the Center of Business Enterprise Development to review for MBE/WBE compliance with the Minority- and Women- owned Business Enterprises (MBE/WBE) Ordinance.

JC/ma

CC: Rosha Brisco, (OCPO)
James Fitzpatrick, (States Attorneys)

I. POLICY AND GOALS

A. It is the policy of the County of Cook to prevent discrimination in the award of or participation in County Contracts and to eliminate arbitrary barriers for participation in such Contracts by local businesses certified as a Minority Business Enterprise (MBE) and Women-owned Business Enterprise (WBE) as both prime and sub-contractors. In furtherance of this policy, the Cook County Board of Commissioners has adopted a Minority- and Women-owned Business Enterprise Ordinance (the "Ordinance") which establishes annual goals for MBE and WBE participation as outlined below:

Contract Type	**Goals**	
	MBE	**WBE**
Goods and Services	25%	10%
Construction	24%	10%
Professional Services	35% Overall	

B. **The County shall set contract-specific goals, based on the availability of MBEs and WBEs that are certified to provide commodities or services specified in this solicitation document. The MBE/WBE participation goals for this Agreement is zero percent (0%).** A Bid, Quotation, or Proposal shall be rejected if the County determines that it fails to comply with this General Condition in any way, including but not limited to: (i) failing to state an enforceable commitment to achieve for this contract the identified MBE/WBE Contract goals; or (ii) failing to include a Petition for Reduction/Waiver, which states that the goals for MBE/WBE participation are not attainable despite the Bidder or Proposer Good Faith Efforts, and explains why. If a Bid, Quotation, or Proposal is rejected, then a new Bid, Quotation, or Proposal may be solicited if the public interest is served thereby.

C. To the extent that a Bid, Quotation, or Proposal includes a Petition for Reduction/Waiver that is approved by the Office of Contract Compliance, the Contract specific MBE and WBE participation goals may be achieved by the proposed Bidder or Proposer's status as an MBE or WBE; by the Bidder or Proposer's enforceable joint-venture agreement with one or more MBEs and/or WBEs; by the Bidder or Proposer entering into one or more enforceable subcontracting agreements with one or more MBE and WBE; by the Bidder or Proposer establishing and carrying out an enforceable mentor/protégé agreement with one or more MBE and WBE; by the Bidder or Proposer actively engaging the Indirect Participation of one or more MBE and WBE in other aspects of its business; or by any combination of the foregoing, so long as the Utilization Plan evidences a commitment to meet the MBE and WBE Contract goals set forth in (B) above, as approved by the Office of Contract Compliance.

D. A single Person, as defined in the Procurement Code, may not be utilized as both an MBE and a WBE on the same Contract, whether as a Consultant, Subcontractor or supplier.

E. Unless specifically waived in the Bid or Proposal Documents, this Exhibit; the Ordinance; and the policies and procedures promulgated thereunder shall govern. If there is a conflict

between this Exhibit and the Ordinance or the policies and procedures, the Ordinance shall control.

F. A Consultant's failure to carry out its commitment regarding MBE and WBE participation in the course of the Contract's performance may constitute a material breach of the Contract. If such breach is not appropriately cured, it may result in withholding of payments under the Contract, contractual penalties, disqualification and any other remedy provided for in Division 4 of the Procurement Code at law or in equity.

II. REQUIRED BID OR PROPOSAL SUBMITTALS

A Bidder or Proposer shall document its commitment to meeting the Contract specific MBE and WBE participation goals by submitting a Utilization Plan with the Bid or Proposal. The Utilization Plan shall include (1) one or more Letter(s) of Intent from the relevant MBE and WBE firms; and (2) current Letters of Certification as an MBE or WBE. Alternatively, the Bidder or Proposer shall submit (1) a written Petition for Reduction/Waiver with the Bid, Quotation or Proposal, which documents its preceding Good Faith Efforts and an explanation of its inability to meet the goals for MBE and WBE participation. The Utilization Plan shall be submitted at the time that the bid or proposal is due. **Failure to include a Utilization Plan will render the submission not Responsive and shall be cause for the CPO to reject the Bid or Proposal.**

A. MBE/WBE Utilization Plan

Each Bid or Proposal shall include a complete Utilization Plan, as set forth on Form 1 of the M/WBE Compliance Forms. The Utilization Plan shall include the name(s), mailing address, email address, and telephone number of the principal contact person of the relevant MBE and WBE firms. If the Bidder or Proposer submits a Bid or Proposal, and any of their subconsultants, suppliers or consultants, are certified MBE or WBE firms, they shall be identified as an MBE or WBE within the Utilization Plan.

1. Letter(s) of Intent

Except as set forth below, a Bid or Proposal shall include, as part of the Utilization Plan, one or more Letter(s) of Intent, as set forth on Form 2 of the M/WBE Compliance Forms, executed by each MBE and WBE and the Bidder or Proposer. The Letter(s) of Intent will be used to confirm that each MBE and WBE shall perform work as a Subcontractor, supplier, joint venture, or consultant on the Contract. Each Letter of Intent shall indicate whether and the degree to which the MBE or WBE will provide goods or services directly or indirectly during the term of the Contract. The box for direct participation shall be marked if the proposed MBE or WBE will provide goods or services directly related to the scope of the Contract. The box for Indirect participation shall be marked if the proposed MBE or WBE will not be directly involved in the Contract but will be utilized by the Bidder or Proposer for other services not related to the Contract. Indirect Participation shall not be counted toward the participation goal. Each Letter of Intent shall accurately detail the work to be performed by the relevant MBE or WBE firm, the agreed dollar amount, the percentage of work, and the terms of payment.

Failure to include Letter(s) of Intent will render the submission not Responsive and shall be cause for the CPO to reject the Bid or Proposal.

All Bids and Proposals must conform to the commitments made in the corresponding Letter(s) of Intent, as may be amended through change orders.

The Contract Compliance Director may at any time request supplemental information regarding Letter(s) of Intent, and such information shall be furnished if the corresponding Bid or Proposal is to be deemed responsive.

2. Letter(s) of Certification

Only current Letter(s) of Certification from one of the following entities may be accepted as proof of certification for MBE/WBE status, provided that Cook County's requirements for certification are met:

- County of Cook
- City of Chicago

Persons that are currently certified by the City of Chicago in any area other than Construction/Public Works shall also complete and submit a MBE/WBE Reciprocal Certification Affidavit along with a current letter of certification from the City of Chicago. This Affidavit form can be downloaded from www.cookcountyil.gov/contractcompliance.

The Contract Compliance Director may reject the certification of any MBE or WBE on the ground that it does not meet the requirements of the Ordinance, or the policies and rules promulgated thereunder.

3. Joint Venture Affidavit

In the event a Bid or Proposal achieves MBE and/or WBE participation through a Joint Venture, the Bid or Proposal shall include the required Joint Venture Affidavit, which can be downloaded from www.cookcountyil.gov/contractcompliance. The Joint Venture Affidavit shall be submitted with the Bid or Proposal, along with current Letter(s) of Certification.

B. Petition for Reduction/Waiver

In the event a Bid or Proposal does not meet the Contract specific goals for MBE and WBE participation, the Bid or Proposal shall include a Petition for Reduction/Waiver, as set forth on Form 3. The Petition for Reduction/Waiver shall be supported by sufficient evidence and documentation to demonstrate the Bidder or Proposer's Good Faith Efforts in attempting to achieve the applicable MBE and WBE goals, and its inability to do so despite its Good Faith Efforts.

Failure to include Petition for Reduction/Waiver will render the submission not Responsive and shall be cause for the CPO to reject the Bid or Proposal.

III. REDUCTION/WAIVER OF MBE/WBE GOALS

A. Granting or Denying a Reduction/Waiver Request.

1. The adequacy of the Good Faith Efforts to utilize MBE and WBE firms in a Bid or Proposal will be evaluated by the CCD under such conditions as are set forth in the Ordinance, the policies and rules promulgated thereunder, and in the "Petition for Reduction/Waiver of MBE/WBE Participation Goals" – Form 3 of the M/WBE Compliance Forms.

2. With respect to a Petition for Reduction/Waiver, the sufficiency or insufficiency of a Bidder or Proposer's Good Faith Efforts shall be evaluated by the CCD as of the date upon which the corresponding Bid or Proposal was due.

3. The Contract Compliance Director or his or her duly authorized Waiver Committee may grant or deny the Petition for Reduction/Waiver based upon factors including but not limited to: (a) whether sufficient qualified MBE and WBE firms are unavailable despite good faith efforts on the part of the Bidder or Proposer; (b) the degree to which specifications and the reasonable and necessary requirements for performing the Contract make it impossible or economically infeasible to divide the Contract into sufficiently small tasks or quantities so as to enable the Bidder or Proposer to utilize MBE and WBE firms in accordance with the applicable goals; (c) the degree to which the prices or prices required by any potential MBE or WBE are more that 10% above competitive levels; and (d) such other factors as are determined relevant by the Contract Compliance Director or the duly authorized Waiver Committee.

4. If the Contract Compliance Director or the duly authorized Waiver Committee determines that the Bidder or Proposer has not demonstrated sufficient Good Faith Efforts to meet the applicable MBE and WBE goals, the Contract Compliance Director or the duly authorized Waiver Committee may deny a Petition for Reduction/Waiver, declare the Bid or Proposal non-responsive, and recommend rejection of the Bid, Quotation, or Proposal.

IV. CHANGES IN CONSULTANT'S UTILIZATION PLAN

A. A Consultant, during its performance of the Contract, may not change the original MBE or WBE commitments specified in the relevant Utilization Plan, including but not limited to, terminating a MBE or WBE Contract, reducing the scope of the work to be performed by a MBE/WBE, or decreasing the price to a MBE/WBE, except as otherwise provided by the Ordinance and according to the policies and procedures promulgated thereunder.

B. Where a Person listed under the Contract was previously considered to be a MBE or WBE but is later found not to be, or work is found not to be creditable toward the MBE or WBE goals as stated in the Utilization Plan, the Consultant shall seek to discharge the disqualified enterprise, upon proper written notification to the Contract Compliance Director, and make every effort to identify and engage a qualified MBE or WBE as its replacement. Failure to obtain an MBE or WBE replacement within 30 business days of the Contract Compliance Director's written approval of the removal of a purported MBE or WBE may result in the termination of the Contract or the imposition of such remedy authorized by the Ordinance, unless a written Petition for Reduction/Waiver is granted allowing the Consultant to award the work to a Person that is not certified as an MBE or WBE.

V. NON-COMPLIANCE

If the CCD determines that the Consultant has failed to comply with its contractual commitments or any portion of the Ordinance, the policies and procedures promulgated thereunder, or this Exhibit, the Contract Compliance Director shall notify the Consultant of such determination and may take any and all appropriate actions as set forth in the Ordinance or the policies and procedures promulgated thereunder which includes but is not limited to disqualification, penalties, withholding of payments or other remedies in law or equity.

VI. REPORTING/RECORD-KEEPING REQUIREMENTS

The Consultant shall comply with the reporting and record-keeping requirements in the manner and time established by the Ordinance, the policies and procedure promulgated thereunder, and the Contract Compliance Director. Failure to comply with such reporting and record-keeping requirements may result in a declaration of Contract default. Upon award of a Contract, a Consultant shall acquire and utilize all Cook County reporting and record-keeping forms and methods which are made available by the Office of Contract Compliance. MBE and WBE firms shall be required to verify payments made by and received from the prime Consultant.

VII. EQUAL EMPLOYMENT OPPORTUNITY

Compliance with MBE and WBE requirements will not diminish or supplant other legal Equal Employment Opportunity and Civil Rights requirements that relate to Consultant and Subcontractor obligations.

Any questions regarding this section should be directed to:
Office of the Chief Procurement Officer, Business Enterprise Development
Cook County
161 N. Clark Street, Suite 2300
Chicago, IL 60601
(312) 603-5502

EXHIBIT 7

Evidence of Insurance

CERTIFICATE OF LIABILITY INSURANCE

DATE(MM/DD/YYYY)
12/02/2025

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).

Holder Identifier :

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:	AIG Specialty Insurance Company	26883
INSURER B:	National Casualty Company	11991
INSURER C:	Scottsdale Ins Company	41297
INSURER D:		
INSURER E:		
INSURER F:		

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

COVERAGES **CERTIFICATE NUMBER:** 570116923433 **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	
B	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
B	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
C	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
B	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
A	E&O - Technology			023593127 Cyber/Tech E&O SIR applies per policy terms & conditions	08/01/2025	08/01/2026	Security/Privacy SIR Policy Limit	$5,000,000 $1,000,000 $5,000,000

Certificate No : 570116923433

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, Workers Compensation, Excess Liability and General Liability policies.

CERTIFICATE HOLDER

Cook County Government
118 N. Clark Street
Chicago IL 60602 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.

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: 570116923433	
CARRIER / NAIC CODE	EFFECTIVE DATE:
See Certificate Number: 570116923433	

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

EXHIBIT 8

Board Authorization

Legislation Details (With Text)

File #:	26-0025	**Version:** 1	**Name:**	Axon Enterprise, Inc., Scottsdale, Arizona
Type:	Contract (Technology)		**Status:**	Approved
File created:	11/18/2025		**In control:**	Board of Commissioners
On agenda:	12/18/2025		**Final action:**	12/18/2025
Title:	PROPOSED CONTRACT (TECHNOLOGY)			

Department(s): Cook County State's Attorney's Office

Vendor: Axon Enterprise, Inc., Scottsdale, Arizona

Request: Authorization for the Chief Procurement Officer to enter into and execute contract

Good(s) or Service(s): Digital Evidence Management System and related products

Contract Value: $11,101,643.12 initial five-year term; (renewal options value: $13,543,520.88; first two-year renewal option $5,101,258.39; second two-year renewal option $5,517,521.08; and final one -year renewal option $2,924,741.41).

Contract period: 1/1/2026 - 12/31/2030 with two (2) two-year renewal options and one (1) one-year renewal option

Contract Utilization: The Contract specific goal set on this contract is Zero.

Potential Fiscal Year Budget Impact: FY2026 $2,024,665.93 FY2027 $2,137,537.77, FY2028 $2,223,039.28 FY2029 $2,311,960.85, FY2030 $2,404,439.29; (Renewal Options FY2031 $2,500,616.86, FY2032 $2,600,641.53, FY2033 $2,704,667.20, FY2034 $2,812,853.88 FY2035 $2,924,741.41).

Accounts: FY 2026 - 11601.1250.21120.560225; FY 2027 - FY 2030 11100.1250.14245.540130; and FY 2031 - FY 2035 - 11100.1250.14245.540130.

Contract Number(s): 2526-10211

Concurrence:

BOT abstains from concurring on this procurement as it relates to the unique operations of another elected office.

Summary: The Cook County State's Attorney's Office is requesting authorization for the Chief Procurement Officer to enter, and execute, a contract with Axon Enterprise, Inc., to provide a digital evidence management system.

This contract will allow the State's Attorney's office to replace the existing evidence management system with Axon Enterprise's Justice Premier system to streamline the discover, auditing, and the centralization and organization of multiple types of digital evidence using Evidence.com, and Axon: Investigate for trial support and preparation.

This is a Comparable Government Procurement pursuant to Section 34-140 of the procurement code. Axon Enterprise, Inc. was previously awarded a contract from a competitive Request for Proposals (RFP) process through OMNIA Partners and the University of Nebraska whereas OMNIA Partners is a collaborative purchasing organization servicing public agencies, and its procurements are led by

public procurement agencies. Cook County wishes to leverage this procurement effort.

Sponsors:

Indexes: EILEEN O'NEILL BURKE, Cook County State's Attorney

Code sections:

Attachments:

Date	Ver.	Action By	Action	Result
12/18/2025	1	Board of Commissioners	approve	Pass

PROPOSED CONTRACT (TECHNOLOGY)

Department(s): Cook County State's Attorney's Office

Vendor: Axon Enterprise, Inc., Scottsdale, Arizona

Request: Authorization for the Chief Procurement Officer to enter into and execute contract

Good(s) or Service(s): Digital Evidence Management System and related products

Contract Value: $11,101,643.12 initial five-year term; (renewal options value: $13,543,520.88; first two-year renewal option $5,101,258.39; second two-year renewal option $5,517,521.08; and final one-year renewal option $2,924,741.41).

Contract period: 1/1/2026 - 12/31/2030 with two (2) two-year renewal options and one (1) one-year renewal option

Contract Utilization: The Contract specific goal set on this contract is Zero.

Potential Fiscal Year Budget Impact: FY2026 $2,024,665.93 FY2027 $2,137,537.77, FY2028 $2,223,039.28 FY2029 $2,311,960.85, FY2030 $2,404,439.29; (Renewal Options FY2031 $2,500,616.86, FY2032 $2,600,641.53, FY2033 $2,704,667.20, FY2034 $2,812,853.88 FY2035 $2,924,741.41).

Accounts: FY 2026 - 11601.1250.21120.560225; FY 2027 - FY 2030 11100.1250.14245.540130; and FY 2031 - FY 2035 - 11100.1250.14245.540130.

Contract Number(s): 2526-10211

Concurrence:

BOT abstains from concurring on this procurement as it relates to the unique operations of another elected office.

Summary: The Cook County State's Attorney's Office is requesting authorization for the Chief Procurement Officer to enter, and execute, a contract with Axon Enterprise, Inc., to provide a digital evidence management system.

This contract will allow the State's Attorney's office to replace the existing evidence management system with Axon Enterprise's Justice Premier system to streamline the discover, auditing, and the centralization and organization of multiple types of digital evidence using Evidence.com, and Axon: Investigate for trial support and preparation.

This is a Comparable Government Procurement pursuant to Section 34-140 of the procurement code. Axon Enterprise, Inc. was previously awarded a contract from a competitive Request for Proposals (RFP) process through OMNIA Partners and the University of Nebraska whereas OMNIA Partners is a collaborative purchasing organization servicing public agencies, and its procurements are led by public procurement agencies. Cook County wishes to leverage this procurement effort.

EXHIBIT 9

Identification of Subcontractors/Suppliers/Subconsultants

Contract #: 2526-10211

OCPO ONLY:
☐ Disqualification
☐ Check Complete

Cook County
Office of the Chief Procurement Officer
Identification of Subcontractor/Supplier/Subconsultant Form

The Bidder/Proposer/Respondent ("the Contractor") will fully complete and execute and submit an Identification of Subcontractor/Supplier/Subconsultant Form ("ISF") with each Bid, Request for Proposal, and Request for Qualification. **The Contractor must complete the ISF for each Subcontractor, Supplier or Subconsultant which shall be used on the Contract**. In the event that there are any changes in the utilization of Subcontractors, Suppliers or Subconsultants, the Contractor must file an updated ISF.

Bid/RFP/RFQ No.: 2526-10211	Date: 11/20/2025
Total Bid or Proposal Amount: $ 11,101,643.12	Contract Title: Digital Evidence Management Service
Contractor: Axon Enterprise, Inc.	Subcontractor/Supplier/ Subconsultant to be added or substitute: N/A
Authorized Contact for Contractor: Robert E. Driscoll, Jr.	Authorized Contact for Subcontractor/Supplier/ Subconsultant: N/A
Email Address (Contractor): contracts@axon.com	Email Address (Subcontractor): N/A
Company Address (Contractor): 17800 N. 85th St	Company Address (Subcontractor): N/A
City, State and Zip (Contractor): Scottsdale, AZ 85255-6311	City, State and Zip (Subcontractor): N/A
Telephone and Fax (Contractor): 800-978-2737	Telephone and Fax (Subcontractor): N/A
Estimated Start and Completion Dates (Contractor): 01/01/2026 - 12/31/2030	Estimated Start and Completion Dates (Subcontractor): N/A

Note: Upon request, a copy of all written subcontractor agreements must be provided to the OCPO.

Description of Services or Supplies	**Total Price of Subcontract for Services or Supplies**
N/A	N/A

The subcontract documents will incorporate all requirements of the Contract awarded to the Contractor as applicable. The subcontract will in no way hinder the Subcontractor/Supplier/Subconsultant from maintaining its progress on any other contract on which it is either a Subcontractor/Supplier/Subconsultant or principal contractor. This disclosure is made with the understanding that the Contractor is not under any circumstances relieved of its abilities and obligations, and is responsible for the organization, performance, and quality of work. **This form does not approve any proposed changes, revisions or modifications to the contract approved MBE/WBE Utilization Plan. Any changes to the contract's approved MBE/WBE/Utilization Plan must be submitted to the Office of the Contract Compliance.**

Axon Enterprise, Inc.
Contractor

Robert E. Driscoll, Jr.
Name

Deputy General Counsel
Title

Signed by: Robert E. Driscoll, Jr. — 11/20/2025 | 4:28 PM MST
Prime Contractor Signature — Date

EXHIBIT 10

Electronic Payables Program ("E-Payables")

OFFICE OF THE COOK COUNTY COMPTROLLER
ELECTRONIC PAYABLES PROGRAM ("E-PAYABLES")

FOR INFORMATION PURPOSES ONLY

This document describes the Office of the Cook County Comptroller's Electronic Payables Program ("E-Payables"). If you wish to participate in E-Payables, please contact the Cook County Comptroller's Office, Accounts Payable, 161 N. Clark Street, Suite 1900, Chicago, IL 60601 or epay.support@cookcountyil.gov.

DESCRIPTION
To increase payment efficiency and timeliness, we have introduced E-Payables program, a new payment initiative to our accounts payable model. This new initiative utilizes a Visa purchasing card and operates through the Visa payment network. This is County's preferred method of payment and your participation in our Visa purchasing card program will provide mutual benefits both to your organization and ours.

As a vendor, you may experience the following benefits by accepting this new payment type:
- Improved cash flow and accelerated payment
- Reduced paperwork and a more streamlined accounts receivable process
- Elimination of stop payment issues
- Reduced payment delays
- Reduced costs for handling paper checks
- Payments settled directly to your merchant account

There are two options within this initiative:

1. **Dedicated Credit Card – "PULL" Settlement**

For this option, you will have an assigned dedicated credit card to be used for each payment. You will provide a point of contact within your organization who will keep credit card information on file. Each time a payment is made, you will receive a remittance advice via email detailing the invoices being paid. Each time you receive a remittance advice, you will process payments in the same manner you process credit card transactions today.

2. **One-Time Use Credit Card – "SUGA" Settlement**

For this option, you will provide a point of contact within your organization who will receive an email notification authorizing you to process payments in the same manner you process credit card transactions today. Each time payment is made, you will receive a remittance advice, via email, detailing the invoices being paid. Also, each time you receive a remittance advice, you will receive a new, unique credit card number. This option is ideal for suppliers who are unable to keep credit card account information on file.

REMAINDER OF PAGE INTENTIONALLY LEFT BLANK

Exhibit 11

Economic Disclosure Statement

COOK COUNTY
ECONOMIC DISCLOSURE STATEMENT
AND EXECUTION DOCUMENT
INDEX

SECTION 1
INSTRUCTIONS FOR COMPLETION OF ECONOMIC DISCLOSURE STATEMENT AND EXECUTION DOCUMENT

This Economic Disclosure Statement and Execution Document ("EDS") is to be completed and executed by every Bidder on a County contract, every Proposer responding to a Request for Proposals, and every Respondent responding to a Request for Qualifications, and others as required by the Chief Procurement Officer. The execution of the EDS shall serve as the execution of a contract awarded by the County. The Chief Procurement Officer reserves the right to request that the Bidder or Proposer, or Respondent provide an updated EDS on an annual basis.

Definitions. Terms used in this EDS and not otherwise defined herein shall have the meanings given to such terms in the Instructions to Bidders, General Conditions, Request for Proposals, Request for Qualifications, as applicable.

Affiliate means a person that directly or indirectly through one or more intermediaries, Controls is Controlled by, or is under common Control with the Person specified.

Applicant means a person who executes this EDS.

Bidder means any person who submits a Bid.

Code means the Code of Ordinances, Cook County, Illinois available on municode.com.

Contract shall include any written document to make Procurements by or on behalf of Cook County.

Contractor or *Contracting Party* means a person that enters into a Contract with the County.

Control means the unfettered authority to directly or indirectly manage governance, administration, work, and all other aspects of a business.

EDS means this complete Economic Disclosure Statement and Execution Document, including all sections listed in the Index and any attachments.

Joint Venture means an association of two or more Persons proposing to perform a for-profit business enterprise. Joint Ventures must have an agreement in writing specifying the terms and conditions of the relationship between the partners and their relationship and respective responsibility for the Contract

Lobby or lobbying means to, for compensation, attempt to influence a County official or County employee with respect to any County matter.

Lobbyist means any person who lobbies.

Person or *Persons* means any individual, corporation, partnership, Joint Venture, trust, association, Limited Liability Company, sole proprietorship or other legal entity.

Prohibited Acts means any of the actions or occurrences which form the basis for disqualification under the Code, or under the Certifications hereinafter set forth.

Proposal means a response to an RFP.

Proposer means a person submitting a Proposal.

Response means response to an RFQ.

Respondent means a person responding to an RFQ.

RFP means a Request for Proposals issued pursuant to this Procurement Code.

RFQ means a Request for Qualifications issued to obtain the qualifications of interested parties.

INSTRUCTIONS FOR COMPLETION OF ECONOMIC DISCLOSURE STATEMENT AND EXECUTION DOCUMENT

Section 1: Instructions. Section 1 sets forth the instructions for completing and executing this EDS.

Section 2: Certifications. Section 2 sets forth certifications that are required for contracting parties under the Code and other applicable laws. Execution of this EDS constitutes a warranty that all the statements and certifications contained, and all the facts stated, in the Certifications are true, correct and complete as of the date of execution.

Section 3: Economic and Other Disclosures Statement. Section 3 is the County's required Economic and Other Disclosures Statement form. Execution of this EDS constitutes a warranty that all the information provided in the EDS is true, correct and complete as of the date of execution, and binds the Applicant to the warranties, representations, agreements and acknowledgements contained therein.

Required Updates. The Applicant is required to keep all information provided in this EDS current and accurate. In the event of any change in the information provided, including but not limited to any change which would render inaccurate or incomplete any certification or statement made in this EDS, the Applicant shall supplement this EDS up to the time the County takes action, by filing an amended EDS or such other documentation as is required.

Additional Information. The County's Governmental Ethics and Campaign Financing Ordinances impose certain duties and obligations on persons or entities seeking County contracts, work, business, or transactions, and the Applicant is expected to comply fully with these ordinances. For further information please contact the Director of Ethics at (312) 603-4304 (69 W. Washington St. Suite 3040, Chicago, IL 60602) or visit the web-site at cookcountyil.gov/ethics-board-of.

Authorized Signers of Contract and EDS Execution Page. If the Applicant is a corporation, the President and Secretary must execute the EDS. In the event that this EDS is executed by someone other than the President, attach hereto a certified copy of that section of the Corporate By-Laws or other authorization by the Corporation, satisfactory to the County that permits the person to execute EDS for said corporation. If the corporation is not registered in the State of Illinois, a copy of the Certificate of Good Standing from the state of incorporation must be submitted with this Signature Page.

If the Applicant is a partnership or joint venture, all partners or joint venturers must execute the EDS, unless one partner or joint venture has been authorized to sign for the partnership or joint venture, in which case, the partnership agreement, resolution or evidence of such authority satisfactory to the Office of the Chief Procurement Officer must be submitted with this Signature Page.

If the Applicant is a member-managed LLC all members must execute the EDS, unless otherwise provided in the operating agreement, resolution or other corporate documents. If the Applicant is a manager-managed LLC, the manager(s) must execute the EDS. The Applicant must attach either a certified copy of the operating agreement, resolution or other authorization, satisfactory to the County, demonstrating such person has the authority to execute the EDS on behalf of the LLC. If the LLC is not registered in the State of Illinois, a copy of a current Certificate of Good Standing from the state of incorporation must be submitted with this Signature Page.

If the Applicant is a Sole Proprietorship, the sole proprietor must execute the EDS.

A "Partnership" "Joint Venture" or "Sole Proprietorship" operating under an Assumed Name must be registered with the Illinois county in which it is located, as provided in 805 ILCS 405 (2012), and documentation evidencing registration must be submitted with the EDS.

Effective October 1, 2016 all foreign corporations and LLCs must be registered with the Illinois Secretary of State's Office unless a statutory exemption applies to the applicant. Applicants who are exempt from registering must provide a written statement explaining why they are exempt from registering as a foreign entity with the Illinois Secretary of State's Office.

SECTION 2

CERTIFICATIONS

THE FOLLOWING CERTIFICATIONS ARE MADE PURSUANT TO STATE LAW AND THE CODE. THE APPLICANT IS CAUTIONED TO CAREFULLY READ THESE CERTIFICATIONS PRIOR TO SIGNING THE SIGNATURE PAGE. SIGNING THE SIGNATURE PAGE SHALL CONSTITUTE A WARRANTY BY THE APPLICANT THAT ALL THE STATEMENTS, CERTIFICATIONS AND INFORMATION SET FORTH WITHIN THESE CERTIFICATIONS ARE TRUE, COMPLETE AND CORRECT AS OF THE DATE THE SIGNATURE PAGE IS SIGNED. THE APPLICANT IS NOTIFIED THAT IF THE COUNTY LEARNS THAT ANY OF THE FOLLOWING CERTIFICATIONS WERE FALSELY MADE, THAT ANY CONTRACT ENTERED INTO WITH THE APPLICANT SHALL BE SUBJECT TO TERMINATION.

A. PERSONS AND ENTITIES SUBJECT TO DISQUALIFICATION

No person or business entity shall be awarded a contract or sub-contract, for a period of five (5) years from the date of conviction or entry of a plea or admission of guilt, civil or criminal, if that person or business entity:

1) Has been convicted of an act committed, within the State of Illinois, of bribery or attempting to bribe an officer or employee of a unit of state, federal or local government or school district in the State of Illinois in that officer's or employee's official capacity;

2) Has been convicted by federal, state or local government of an act of bid-rigging or attempting to rig bids as defined in the Sherman Anti-Trust Act and Clayton Act. Act. 15 U.S.C. Section 1 *et seq.;*

3) Has been convicted of bid-rigging or attempting to rig bids under the laws of federal, state or local government;

4) Has been convicted of an act committed, within the State, of price-fixing or attempting to fix prices as defined by the Sherman Anti-Trust Act and the Clayton Act. 15 U.S.C. Section 1, *et seq.;*

5) Has been convicted of price-fixing or attempting to fix prices under the laws the State;

6) Has been convicted of defrauding or attempting to defraud any unit of state or local government or school district within the State of Illinois;

7) Has made an admission of guilt of such conduct as set forth in subsections (1) through (6) above which admission is a matter of record, whether or not such person or business entity was subject to prosecution for the offense or offenses admitted to; or

8) Has entered a plea of *nolo contendere* to charge of bribery, price-fixing, bid-rigging, or fraud, as set forth in sub-paragraphs (1) through (6) above.

In the case of bribery or attempting to bribe, a business entity may not be awarded a contract if an official, agent or employee of such business entity committed the Prohibited Act on behalf of the business entity and pursuant to the direction or authorization of an officer, director or other responsible official of the business entity, and such Prohibited Act occurred within three years prior to the award of the contract. In addition, a business entity shall be disqualified if an owner, partner or shareholder controlling, directly or indirectly, 20% or more of the business entity, or an officer of the business entity has performed any Prohibited Act within five years prior to the award of the Contract.

THE APPLICANT HEREBY CERTIFIES THAT: The Applicant has read the provisions of Section A, Persons and Entities Subject to Disqualification, that the Applicant has not committed any Prohibited Act set forth in Section A, and that award of the Contract to the Applicant would not violate the provisions of such Section or of the Code.

B. BID-RIGGING OR BID ROTATING

THE APPLICANT HEREBY CERTIFIES THAT: *In accordance with 720 ILCS 5/33 E-11, neither the Applicant nor any Affiliated Entity is barred from award of this Contract as a result of a conviction for the violation of State laws prohibiting bid-rigging or bid rotating.*

C. DRUG FREE WORKPLACE ACT

THE APPLICANT HEREBY CERTIFIES THAT: The Applicant will provide a drug free workplace, as required by (30 ILCS 580/3).

D. DELINQUENCY IN PAYMENT OF TAXES

***THE APPLICANT HEREBY CERTIFIES THAT**: The Applicant is not an owner or a party responsible for the payment of any tax or fee administered by Cook County, such as bar award of a contract or subcontract pursuant to the Code, Chapter 34, Section 34-171.*

E. HUMAN RIGHTS ORDINANCE

No person who is a party to a contract with Cook County ("County") shall engage in unlawful discrimination or sexual harassment against any individual in the terms or conditions of employment, credit, public accommodations, housing, or provision of County facilities, services or programs (Code Chapter 42, Section 42-30 *et seq.*).

F. ILLINOIS HUMAN RIGHTS ACT

***THE APPLICANT HEREBY CERTIFIES THAT:** It is in compliance with the Illinois Human Rights Act (775 ILCS 5/2-105), and agrees to abide by the requirements of the Act as part of its contractual obligations.*

G. INSPECTOR GENERAL (COOK COUNTY CODE, CHAPTER 34, SECTION 34-174 and Section 34-250)

The Applicant has not willfully failed to cooperate in an investigation by the Cook County Independent Inspector General or to report to the Independent Inspector General any and all information concerning conduct which they know to involve corruption, or other criminal activity, by another county employee or official, which concerns his or her office of employment or County related transaction.

The Applicant has reported directly and without any undue delay any suspected or known fraudulent activity in the County's Procurement process to the Office of the Cook County Inspector General.

H. CAMPAIGN CONTRIBUTIONS (COOK COUNTY CODE, CHAPTER 2, SECTION 2-585)

THE APPLICANT CERTIFIES THAT: It has read and shall comply with the Cook County's Ordinance concerning campaign contributions, which is codified at Chapter 2, Division 2, Subdivision II, Section 585, and can be read in its entirety at www.municode.com.

I. GIFT BAN, (COOK COUNTY CODE, CHAPTER 2, SECTION 2-574)

THE APPLICANT CERTIFIES THAT: It has read and shall comply with the Cook County's Ordinance concerning receiving and soliciting gifts and favors, which is codified at Chapter 2, Division 2, Subdivision II, Section 574, and can be read in its entirety at www.municode.com.

J. LIVING WAGE ORDINANCE PREFERENCE (COOK COUNTY CODE, CHAPTER 34, SECTION 34-160;

Unless expressly waived by the Cook County Board of Commissioners, the Code requires that a living wage must be paid to individuals employed by a Contractor which has a County Contract and by all subcontractors of such Contractor under a County Contract, throughout the duration of such County Contract. The amount of such living wage is annually by the Chief Financial Officer of the County, and shall be posted on the Chief Procurement Officer's website.

The term "Contract" as used in Section 4, I, of this EDS, specifically excludes contracts with the following:

1) Not-For Profit Organizations (defined as a corporation having tax exempt status under Section 501(C)(3) of the United State Internal Revenue Code and recognized under the Illinois State not-for -profit law);

2) Community Development Block Grants;

3) Cook County Works Department;

4) Sheriff's Work Alternative Program; and

5) Department of Correction inmates.

SECTION 3

REQUIRED DISCLOSURES

1. DISCLOSURE OF LOBBYIST CONTACTS

List all persons that have made lobbying contacts on your behalf with respect to this contract:

Name Address

N/A

2. LOCAL BUSINESS PREFERENCE STATEMENT (CODE, CHAPTER 34, SECTION 34-230)

Local business means a Person, including a foreign corporation authorized to transact business in Illinois, having a bona fide establishment located within the County at which it is transacting business on the date when a Bid is submitted to the County, and which employs the majority of its regular, full-time work force within the County. A Joint Venture shall constitute a Local Business if one or more Persons that qualify as a "Local Business" hold interests totaling over 50 percent in the Joint Venture, even if the Joint Venture does not, at the time of the Bid submittal, have such a bona fide establishment within the County.

a) Is Applicant a "Local Business" as defined above?

Yes: ☐ No: ☑

b) If yes, list business addresses within Cook County:

c) Does Applicant employ the majority of its regular full-time workforce within Cook County?

Yes: ☐ No: ☑

3. THE CHILD SUPPORT ENFORCEMENT ORDINANCE (CODE, CHAPTER 34, SECTION 34-172)

Every Applicant for a County Privilege shall be in full compliance with any child support order before such Applicant is entitled to receive or renew a County Privilege. When delinquent child support exists, the County shall not issue or renew any County Privilege, and may revoke any County Privilege.

All Applicants are required to review the Cook County Affidavit of Child Support Obligations attached to this EDS (EDS-5) and complete the Affidavit, based on the instructions in the Affidavit.

4. REAL ESTATE OWNERSHIP DISCLOSURES.

The Applicant must indicate by checking the appropriate provision below and providing all required information that either:

a) The following is a complete list of all real estate owned by the Applicant in Cook County:

PERMANENT INDEX NUMBER(S): _____

_____

_____

(ATTACH SHEET IF NECESSARY TO LIST ADDITIONAL INDEX NUMBERS)

OR:

b) ☑ The Applicant owns no real estate in Cook County.

5. EXCEPTIONS TO CERTIFICATIONS OR DISCLOSURES.

If the Applicant is unable to certify to any of the Certifications or any other statements contained in this EDS and not explained elsewhere in this EDS, the Applicant must explain below:

If the letters, "NA", the word "None" or "No Response" appears above, or if the space is left blank, it will be conclusively presumed that the Applicant certified to all Certifications and other statements contained in this EDS.

COOK COUNTY DISCLOSURE OF OWNERSHIP INTEREST STATEMENT

The Cook County Code of Ordinances (§2-610 *et seq.*) requires that any Applicant for any County Action must disclose information concerning ownership interests in the Applicant. This Disclosure of Ownership Interest Statement must be completed with all information current as of the date this Statement is signed. Furthermore, this Statement must be kept current, by filing an amended Statement, until such time as the County Board or County Agency shall take action on the application. The information contained in this Statement will be maintained in a database and made available for public viewing. **County reserves the right to request additional information to verify veracity of information contained in this statement.**

If you are asked to list names, but there are no applicable names to list, you must state NONE. An incomplete Statement will be returned and any action regarding this contract will be delayed. A failure to fully comply with the ordinance may result in the action taken by the County Board or County Agency being voided.

"*Applicant*" means any Entity or person making an application to the County for any County Action.

"County Action" means any action by a County Agency, a County Department, or the County Board regarding an ordinance or ordinance amendment, a County Board approval, or other County agency approval, with respect to contracts, leases, or sale or purchase of real estate.

"Person" "Entity" or *"Legal Entity"* means a sole proprietorship, corporation, partnership, association, business trust, estate, two or more persons having a joint or common interest, trustee of a land trust, other commercial or legal entity or any beneficiary or beneficiaries thereof.

This Disclosure of Ownership Interest Statement must be submitted by :

1. An Applicant for County Action and

2. A Person that holds stock or a beneficial interest in the Applicant and is listed on the Applicant's Statement (a "Holder") must file a Statement and complete #1 only under **Ownership Interest Declaration**.

Please print or type responses clearly and legibly. Add additional pages if needed, being careful to identify each portion of the form to which each additional page refers.

This Statement is being made by the [✓] Applicant or [ ] Stock/Beneficial Interest Holder

This Statement is an: [ ] Original Statement or [ ] Amended Statement

Identifying Information:

Name Axon Enterprise, Inc.

D/B/A: _____ FEIN # Only: 86-0871227

Street Address: 17800 N. 85th Street

City: Scottsdale State: AZ Zip Code: 85255

Phone No.: 800-978-2737 Fax Number: 480-991-0791 Email: contracts@axon.com

Cook County Business Registration Number: _____
(Sole Proprietor, Joint Venture Partnership)

Corporate File Number (if applicable): Illinois Certificate of Registration Account ID: 4151-9159

Form of Legal Entity:

[ ] Sole Proprietor [ ] Partnership [✓] Corporation [ ] Trustee of Land Trust

[ ] Business Trust [ ] Estate [ ] Association [ ] Joint Venture

[ ] Other (describe) _____

Ownership Interest Declaration:

1. List the name(s), address, and percent ownership of each Person having a legal or beneficial interest (including ownership) of more than five percent (5%) in the Applicant/Holder.

Name	Address	Percentage Interest in Applicant/Holder
Vanguard Group, Inc.	100 Vanguard Blvd., Malvern, PA 19355	11.86%
BlackRock, Inc.	55 East 2nd Street, New York, NY 10022	8.20%

2. If the interest of any Person listed in (1) above is held as an agent or agents, or a nominee or nominees, list the name and address of the principal on whose behalf the interest is held.

Name of Agent/Nominee	Name of Principal	Principal's Address
N/A		

3. Is the Applicant constructively controlled by another person or Legal Entity? [☐] Yes [☑] No

If yes, state the name, address and percentage of beneficial interest of such person, and the relationship under which such control is being or may be exercised.

Name	Address	Percentage of Beneficial Interest	Relationship

Corporate Officers, Members and Partners Information:

For all corporations, list the names, addresses, and terms for all corporate officers. For all limited liability companies, list the names, addresses for all members. For all partnerships and joint ventures, list the names, addresses, for each partner or joint venture.

Name	Address	Title (specify title of Office, or whether manager or partner/joint venture)	Term of Office
Patrick Smith	17800 N. 85th Street, Scottsdale, AZ 85255	Chief Executive Officer	Indefinite
Josh Isner	17800 N. 85th Street, Scottsdale, AZ 85255	President	Indefinite
Brittany Bagley	17800 N. 85th Street, Scottsdale, AZ 85255	Chief Operating Officer & CFO	Indefinite

Declaration (check the applicable box):

☑ I state under oath that the Applicant has withheld no disclosure as to ownership interest in the Applicant nor reserved any information, data or plan as to the intended use or purpose for which the Applicant seeks County Board or other County Agency action.

☑ I state under oath that the Holder has withheld no disclosure as to ownership interest nor reserved any information required to be disclosed.

COOK COUNTY DISCLOSURE OF OWNERSHIP INTEREST STATEMENT SIGNATURE PAGE

Isaiah Fields
Name of Authorized Applicant/Holder Representative (please print or type)

Chief Legal Officer
Title

Signature

December 8, 2025
Date

contracts@axon.com
E-mail address

800-978-2737
Phone Number

Subscribed to and sworn before me
this 8th day of Dec., 2025.

My commission expires: Sept. 4, 2026

X
Notary Public Signature

Notary Seal

NATALIE SHARP
Notary Public - Arizona
Maricopa County
Commission # 631850
My Comm. Expires Sep 4, 2026

17800 N 85TH STREET
SCOTTSDALE, ARIZONA 85255

AXON.COM

Date: December 23, 2025
RE: Cook County, IL - Disclosure of Ownership Interest Statement exception—The Vanguard Group and Blackrock, Inc.

Dear Mrs. Brisco:

This letter is regarding the Disclosure of Ownership Interest Statement (Statement) that Axon Enterprise, Inc. (Axon) provided to Cook County. Axon respectfully requests an exception to the requirement under Cook County Code Section 1-13-3.B.1 that The Vanguard Group, Inc. (Vanguard) and Blackrock, Inc. (Blackrock) complete its own Statement.

Axon is a publicly listed company that trades on the Nasdaq stock exchange under the AXON ticker. The information we have about Axon's stockholders and beneficial interest holders comes from filings on form 13F, which investment companies must file quarterly with the Securities and Exchange Commission (SEC). We generally rely on a third party, Nasdaq, to summarize these filings and provide us with our most up-to-date ownership information.

Vanguard
Vanguard is a substantial owner of Axon stock, according to a 13F filing that Vanguard made with the SEC on October 30, 2025, which is the latest available. Vanguard lists its address as 100 Vanguard Blvd., Malvern, PA 19355. According to its latest 13F form, Vanguard owns 9,314,070 shares of Axon. This represents approximately 11.86 % of our diluted shares outstanding of 79.4 million shares as of December 2025.

Vanguard is one of the world's largest investment management companies and manages about $10.1 trillion in global assets. At $600 per share of AAXN, the value of Vanguard's ownership of Axon stock is approximately $5.6 billion. This means that Vanguard's ownership of Axon represents 0.057% of its total $15.1 trillion in holdings.

Blackrock
Blackrock is also a substantial owner of Axon stock according to a 13F filing that Blackrock made with the SEC on April 23, 2025, which is the latest available. Blackrock lists its address as 50 Hudson Yards New York, NY 10001. According to its latest 13F form, Blackrock owns 6,401,225 shares of Axon. This represents 8.2% of our diluted shares outstanding of 79.4 million shares as of December 2025.

Blackrock is one of the world's largest investment management companies and manages about $13.46 trillion in global assets. At $600 per share of AAXN, the value of Blackrock's ownership of Axon stock is approximately

17800 N 85TH STREET
SCOTTSDALE, ARIZONA 85255

AXON.COM

$3.8 billion. This means that Blackrock's ownership of Axon represents 0.03% of its total $13.46 trillion in holdings.
Given that Axon represents such a tiny portion of both Vanguard's and Blackrock's total holdings and given that Vanguard's and Blackrock's ownership of Axon is considered passive—that is, computerized buying and selling that track an index fund or a basket of related investments—we do not have a close direct relationship with any individual asset manager at Vanguard or Blackrock. For these reasons, Axon requests this exception. Please see attached Exhibit A, with links to supporting information.

Exhibit A Section 6-7 includes Vanguard's available information for the Ownership Interest Disclosure and Sections 8-9 includes Blackrock's information for the Ownership Disclosure Statement.

Axon is unable to provide ownership information for Vanguard since it is a private company and not required to file such information in addition, Vanguard is uniquely structured so that it is owned by its funds rather than individual investors directly.

Thank you for your time and consideration in this matter. If you have any additional questions, please do not hesitate to contact us.

Regards,

Joshua Campbell
Sr. Corporate Counsel
Axon Enterprise, Inc.

17800 N 85TH STREET
SCOTTSDALE, ARIZONA 85255

AXON.COM

Exhibit A

1. Vanguard website: https://www.ch.vanguard/content/dam/intl/europe/documents/en/vanguard-in-a-nutshell-eu-en.pdf

2. Vanguard 13 F filing: https://www.sec.gov/Archives/edgar/data/102909/000010290925000037/xslSCHEDULE_13G_X01/primary_doc.xml

3. Blackrock holdings as reported by Reuters: https://www.reuters.com/business/blackrocks-assets-hit-record-1346-trillion-third-quarter-markets-rally-2025-10-14/

4. Blackrock 13F filing: https://www.sec.gov/Archives/edgar/data/1069183/000205211325001475/xslSCHEDULE_13G_X01/primary_doc.xml

5. Axon's outstanding shares as reported by yahoo!finance: https://finance.yahoo.com/quote/AXON/key-statistics/

6. **From Form 5500 Schedule C:**

For these purposes, Vanguard's information is as follows:

Name:	The Vanguard Group, Inc.
Address:	P.O. Box 2900 Valley Forge, PA 19482-2900
EIN:	23-1945930

7. **Vanguard Ownership Organization**
https://corporate.vanguard.com/content/corporatesite/us/en/corp/who-we-are/sets-us-apart/ethics-and-integrity.html

AXON

17800 N 85TH STREET
SCOTTSDALE, ARIZONA 85255

AXON.COM

Our approach

Unique ownership structure

Vanguard is owned by its U.S. funds, which in turn are owned by their shareholders. There are no other parties seeking to profit from the management of our funds. The ethical standards, values, and investment principles to which we've adhered since our founding are designed to serve the interests of our clients, communities, and employees.

8. **Blackrock 10-Q Company information**: https://d18rn0p25nwr6d.cloudfront.net/CIK-0002012383/ee909254-7750-42eb-95a3-2f76cb2bdb1a.pdf

UNITED STATES
SECURITIES AND EXCHANGE COMMISSION
WASHINGTON, D.C. 20549

FORM 10-Q

(Mark One)

☒ QUARTERLY REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934.
For the quarterly period ended September 30, 2025

OR

☐ TRANSITION REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934.
For the transition period from _____ to _____.
Commission file number 001-42297

BlackRock

BlackRock, Inc.
(Exact name of registrant as specified in its charter)

Delaware	99-1116001
(State or Other Jurisdiction of Incorporation or Organization)	(I.R.S. Employer Identification No.)

50 Hudson Yards, New York, NY 10001
(Address of Principal Executive Offices) (Zip Code)

(212) 810-5800
(Registrant's Telephone Number, Including Area Code)

(Former Name, Former Address and Former Fiscal Year, if Changed Since Last Report)

Securities registered pursuant to Section 12(b) of the Act:

Title of each class	Trading Symbol(s)	Name of each exchange on which registered
Common Stock, $.01 par value	BLK	New York Stock Exchange
3.750% Notes due 2035	BLK 35	New York Stock Exchange

Indicate by check mark whether the registrant: (1) has filed all reports required to be filed by Section 13 or 15(d) of the Securities Exchange Act of 1934 during

17800 N 85TH STREET
SCOTTSDALE, ARIZONA 85255

AXON.COM

9. **Blackrock Proxy Statement 2025 (Ownership Disclosure):** https://s24.q4cdn.com/856567660/files/doc_financials/2025/ar/PRO013216_91_Blackrock_Proxy-Statement-2025.pdf

As of March 28, 2025, there were 155,022,282 shares of BlackRock common stock outstanding.

	Amount of Beneficial Ownership of Common Stock[1]	Percent of Common Stock Outstanding	Deferred/ Restricted Stock Units and Stock Options[2]	Total
The Vanguard Group, Inc. 100 Vanguard Blvd. Malvern, PA 19355	12,890,008[3]	8.31%	—	12,890,008[3]
BlackRock, Inc. 50 Hudson Yards New York, NY 10001	9,580,403[4]	6.18%	—	9,580,403[4]
Kuwait Investment Authority, acting for and on behalf of the Government of the State of Kuwait Ministries Complex, Block 3 Safat, Kuwait 13001	7,993,064[5]	5.16%	—	7,993,064[5]

COOK COUNTY BOARD OF ETHICS
69 W. WASHINGTON STREET, SUITE 3040
CHICAGO, ILLINOIS 60602
312/603-4304 Office 312/603-9988 Fax

FAMILIAL RELATIONSHIP DISCLOSURE PROVISION

Nepotism Disclosure Requirement:

Doing a significant amount of business with the County requires that you disclose to the Board of Ethics the existence of any familial relationships with any County employee or any person holding elective office in the State of Illinois, the County, or in any municipality within the County. The Ethics Ordinance defines a significant amount of business for the purpose of this disclosure requirement as more than $25,000 in aggregate County leases, contracts, purchases or sales in any calendar year.

If you are unsure of whether the business you do with the County or a County agency will cross this threshold, err on the side of caution by completing the attached familial disclosure form because, among other potential penalties, any person found guilty of failing to make a required disclosure or knowingly filing a false, misleading, or incomplete disclosure will be prohibited from doing any business with the County for a period of three years. The required disclosure should be filed with the Board of Ethics by January 1 of each calendar year in which you are doing business with the County and again with each bid/proposal/quotation to do business with Cook County. The Board of Ethics may assess a late filing fee of $100 per day after an initial 30-day grace period.

The person that is doing business with the County must disclose his or her familial relationships. If the person on the County lease or contract or purchasing from or selling to the County is a business entity, then the business entity must disclose the familial relationships of the individuals who are and, during the year prior to doing business with the County, were:

- its board of directors,
- its officers,
- its employees or independent contractors responsible for the general administration of the entity,
- its agents authorized to execute documents on behalf of the entity, and
- its employees who directly engage or engaged in doing work with the County on behalf of the entity.

Do not hesitate to contact the Board of Ethics at (312) 603-4304 for assistance in determining the scope of any required familial relationship disclosure.

Additional Definitions:

"*Familial relationship*" means a person who is a spouse, domestic partner or civil union partner of a County employee or State, County or municipal official, or any person who is related to such an employee or official, whether by blood, marriage or adoption, as a:

- ☐ Parent
- ☐ Child
- ☐ Brother
- ☐ Sister
- ☐ Aunt
- ☐ Uncle
- ☐ Niece
- ☐ Nephew
- ☐ Grandparent
- ☐ Grandchild
- ☐ Father-in-law
- ☐ Mother-in-law
- ☐ Son-in-law
- ☐ Daughter-in-law
- ☐ Brother-in-law
- ☐ Sister-in-law
- ☐ Stepfather
- ☐ Stepmother
- ☐ Stepson
- ☐ Stepdaughter
- ☐ Stepbrother
- ☐ Stepsister
- ☐ Half-brother
- ☐ Half-sister

COOK COUNTY BOARD OF ETHICS
FAMILIAL RELATIONSHIP DISCLOSURE FORM

A. PERSON DOING OR SEEKING TO DO BUSINESS WITH THE COUNTY

Name of Person Doing Business with the County: Axon Enterprise Inc.

Address of Person Doing Business with the County: 17800 N. 85th Street, Scottsdale, AZ 85255

Phone number of Person Doing Business with the County: 800-978-2737

Email address of Person Doing Business with the County: contracts@axon.com

If Person Doing Business with the County is a Business Entity, provide the name, title and contact information for the individual completing this disclosure on behalf of the Person Doing Business with the County:
Natalie Sharp, Conracts Administrator, nsharp@axon.com

B. DESCRIPTION OF BUSINESS WITH THE COUNTY
Append additional pages as needed and for each County lease, contract, purchase or sale sought and/or obtained during the calendar year of this disclosure (or the proceeding calendar year if disclosure is made on January 1), identify:

The lease number, contract number, purchase order number, request for proposal number and/or request for qualification number associated with the business you are doing or seeking to do with the County: 2526-10211

The aggregate dollar value of the business you are doing or seeking to do with the County: $11,101,643.12

The name, title and contact information for the County official(s) or employee(s) involved in negotiating the business you are doing or seeking to do with the County: Rosha Brisco, rosha.brisco@cookcountyil.gov

The name, title and contact information for the County official(s) or employee(s) involved in managing the business you are doing or seeking to do with the County: James Fitzpatrick, James.fitzpatrick@cookcountysao.org

C. DISCLOSURE OF FAMILIAL RELATIONSHIPS WITH COUNTY EMPLOYEES OR STATE, COUNTY OR MUNICIPAL ELECTED OFFICIALS

Check the box that applies and provide related information where needed

☐ The Person Doing Business with the County **is an individual** and there is **no familial relationship** between this individual and any Cook County employee or any person holding elective office in the State of Illinois, Cook County, or any municipality within Cook County.

☒ The Person Doing Business with the County **is a business entity** and there is **no familial relationship** between any member of this business entity's board of directors, officers, persons responsible for general administration of the business entity, agents authorized to execute documents on behalf of the business entity or employees directly engaged in contractual work with the County on behalf of the business entity, and any Cook County employee or any person holding elective office in the State of Illinois, Cook County, or any municipality within Cook County.

COOK COUNTY BOARD OF ETHICS
FAMILIAL RELATIONSHIP DISCLOSURE FORM

☐ The Person Doing Business with the County **is an individual** and **there is a familial relationship** between this individual and at least one Cook County employee and/or a person or persons holding elective office in the State of Illinois, Cook County, and/or any municipality within Cook County. **The familial relationships are as follows:**

Name of Individual Doing Business with the County	Name of Related County Employee or State, County or Municipal Elected Official	Title and Position of Related County Employee or State, County or Municipal Elected Official	Nature of Familial Relationship*

If more space is needed, attach an additional sheet following the above format.

☐ The Person Doing Business with the County **is a business entity** and **there is a familial relationship** between at least one member of this business entity's board of directors, officers, persons responsible for general administration of the business entity, agents authorized to execute documents on behalf of the business entity and/or employees directly engaged in contractual work with the County on behalf of the business entity, on the one hand, and at least one Cook County employee and/or a person holding elective office in the State of Illinois, Cook County, and/or any municipality within Cook County, on the other. **The familial relationships are as follows:**

Name of Member of Board of Director for Business Entity Doing Business with the County	Name of Related County Employee or State, County or Municipal Elected Official	Title and Position of Related County Employee or State, County or Municipal Elected Official	Nature of Familial Relationship*

Name of Officer for Business Entity Doing Business with the County	Name of Related County Employee or State, County or Municipal Elected Official	Title and Position of Related County Employee or State, County or Municipal Elected Official	Nature of Familial Relationship*

Name of Person Responsible for the General Administration of the Business Entity Doing Business with the County	Name of Related County Employee or State, County or Municipal Elected Official	Title and Position of Related County Employee or State, County or Municipal Elected Official	Nature of Familial Relationship*

Name of Agent Authorized to Execute Documents for Business Entity Doing Business with the County	Name of Related County Employee or State, County or Municipal Elected Official	Title and Position of Related County Employee or State, County or Municipal Elected Official	Nature of Familial Relationship*

Name of Employee of Business Entity Directly Engaged in Doing Business with the County	Name of Related County Employee or State, County or Municipal Elected Official	Title and Position of Related County Employee or State, County or Municipal Elected Official	Nature of Familial Relationship*

If more space is needed, attach an additional sheet following the above format.

VERIFICATION: To the best of my knowledge, the information I have provided on this disclosure form is accurate and complete. I acknowledge that an inaccurate or incomplete disclosure is punishable by law, including but not limited to fines and debarment.

Signature of Recipient

December 8, 2025
Date

SUBMIT COMPLETED FORM TO: Cook County Board of Ethics
69 West Washington Street, Suite 3040, Chicago, Illinois 60602
Office (312) 603-4304 – Fax (312) 603-9988
CookCounty.Ethics@cookcountyil.gov

* Spouse, domestic partner, civil union partner or parent, child, sibling, aunt, uncle, niece, nephew, grandparent or grandchild by blood, marriage (*i.e.* in laws and step relations) or adoption.

SECTION 4

COOK COUNTY AFFIDAVIT FOR WAGE THEFT ORDINANCE

Effective May 1, 2015, every Person, ***including Substantial Owners***, seeking a Contract with Cook County must comply with the Cook County Wage Theft Ordinance set forth in Chapter 34, Article IV, Section 179. Any Person/Substantial Owner, who fails to comply with Cook County Wage Theft Ordinance, may request that the Chief Procurement Officer grant a reduction or waiver in accordance with Section 34-179(d).

"*Contract*" means any written document to make Procurements by or on behalf of Cook County.

"*Person*" means any individual, corporation, partnership, Joint Venture, trust, association, limited liability company, sole proprietorship or other legal entity.

"*Procurement*" means obtaining supplies, equipment, goods, or services of any kind.

"*Substantial Owner*" means any person or persons who own or hold a twenty-five percent (25%) or more percentage of interest in any business entity seeking a County Privilege, including those shareholders, general or limited partners, beneficiaries and principals; except where a business entity is an individual or sole proprietorship, Substantial Owner means that individual or sole proprietor.

All Persons/Substantial Owners are required to complete this affidavit and comply with the Cook County Wage Theft Ordinance before any Contract is awarded. Signature of this form constitutes a certification the information provided below is correct and complete, and that the individual(s) signing this form has/have personal knowledge of such information. **County reserves the right to request additional information to verify veracity of information contained in this Affidavit.**

I. Contract Information:

Contract Number: 2526-10211

County Using Agency (requesting Procurement): Cook County State's Attorney's Office

II. Person/Substantial Owner Information:

Person (Corporate Entity Name): Axon Enterprise, Inc.

Substantial Owner Complete Name: _____

FEIN# 86-0741227

[redacted] E-mail address: contracts@axon.com

Street Address: 17800 N. 85th Street

City: Scottsdale State: AZ Zip: 85255

[redacted]

III. Compliance with Wage Laws:

Within the past five years has the Person/Substantial Owner, in any judicial or administrative proceeding, been convicted of, entered a plea, made an admission of guilt or liability, or had an administrative finding made for committing a repeated or willful violation of any of the following laws:

No	*Illinois Wage Payment and Collection Act, 820 ILCS 115/1 et seq.,* ***YES or NO***
No	*Illinois Minimum Wage Act, 820 ILCS 105/1 et seq.,* ***YES or NO***
No	*Illinois Worker Adjustment and Retraining Notification Act, 820 ILCS 65/1 et seq.,* ***YES or NO***
No	*Employee Classification Act, 820 ILCS 185/1 et seq.,* **YES or NO**
No	*Fair Labor Standards Act of 1938, 29 U.S.C. 201, et seq.,* ***YES or NO***
No	*Any comparable state statute or regulation of any state, which governs the payment of wages* ***YES or NO***

If the Person/Substantial Owner answered **"Yes"** to any of the questions above, it is ineligible to enter into a Contract with Cook County, but can request a reduction or waiver under **Section IV.**

IV. Request for Waiver or Reduction

If Person/Substantial Owner answered **"Yes"** to any of the questions above, it may request a reduction or waiver in accordance with Section 34-179(d), provided that the request for reduction of waiver is made on the basis of one or more of the following actions that have taken place:

No — There has been a bona fide change in ownership or Control of the ineligible Person or Substantial Owner. YES or NO

No — Disciplinary action has been taken against the individual(s) responsible for the acts giving rise to the violation. YES or NO

No — Remedial action has been taken to prevent a recurrence of the acts giving rise to the disqualification or default. YES or NO

No — Other factors that the Person or Substantial Owner believe are relevant. YES or NO

The Person/Substantial Owner must submit documentation to support the basis of its request for a reduction or waiver. The Chief Procurement Officer reserves the right to make additional inquiries and request additional documentation.

V. Affirmation

The Person/Substantial Owner affirms that all statements contained in the Affidavit are true, accurate and complete.

Signature: _____ Date: November 20, 2025

Name of Person signing (Print): Robert E. Driscoll, Jr. Title: Deputy General Counsel

Subscribed and sworn to before me this _____ day of November, 20 25

X _____ _____

Notary Public Signature **Notary Seal**

Note: The above information is subject to verification prior to the award of the Contract.

ELIZABETH LUNA
Notary Public - Arizona
Maricopa County
Commission # 663555
My Comm. Expires Mar 25, 2028

SECTION 5

CONTRACT AND EDS EXECUTION PAGE

The Applicant hereby certifies and warrants that all of the statements, certifications and representations set forth in this EDS are true, complete and correct; that the Applicant is in full compliance and will continue to be in compliance throughout the term of the Contract or County Privilege issued to the Applicant with all the policies and requirements set forth in this EDS; and that all facts and information provided by the Applicant in this EDS are true, complete and correct. The Applicant agrees to inform the Chief Procurement Officer in writing if any of such statements, certifications, representations, facts or information becomes or is found to be untrue, incomplete or incorrect during the term of the Contract or County Privilege.

Execution by Corporation

Axon Enterprise, Inc.
Corporation's Name

Brian Fields
President's Printed Name and Signature

800-978-2737
Telephone

contracts@axon.com
Email

Secretary Signature

November 20, 2025
Date

Execution by LLC

LLC Name

*Member/Manager Printed Name and Signature

Date

Telephone and Email

Execution by Partnership/Joint Venture

Partnership/Joint Venture Name

*Partner/Joint Venturer Printed Name and Signature

Date

Telephone and Email

Execution by Sole Proprietorship

Printed Name Signature

Assumed Name (if applicable)

Date

Telephone and Email

Subscribed and sworn to before me this
20th day of November, 2025.

Notary Public Signature

My commission expires:
3/25/28

Notary Seal

ELIZABETH LUNA
Notary Public - Arizona
Maricopa County
Commission # 663555
My Comm. Expires Mar 25, 2028

*If the operating agreement, partnership agreement or governing documents requiring execution by multiple members, managers, partners, or joint venturers, please complete and execute additional Contract and EDS Execution Pages.

SECTION 6
COOK COUNTY SIGNATURE PAGE

ON BEHALF OF THE COUNTY OF COOK, A BODY POLITIC AND CORPORATE OF THE STATE OF ILLINOIS, THIS CONTRACT IS HEREBY EXECUTED BY:

Raffi Sarrafian Digitally signed by Raffi Sarrafian Date: 2025.12.30 11:57:08 -06'00'

Cook County Chief Procurement Officer — Date

APPROVED AS TO FORM:

Brian Tracy — 12/17/2025

Assistant State's Attorney (Required on contracts over $1,000,000 — Date

CONTRACT TERM & AMOUNT

2526-10211
Contract #

January 1, 2026 through December 31, 2030 with two (2), two-year renewal options, and one (1), one-year year renewal option.
Original Contract Term — Renewal Options (If Applicable)

$ 11,101,643.12
Contract Amount

December 18, 2025
Cook County Board Approval Date (If Applicable)

APPROVED BY THE BOARD OF
COOK COUNTY COMMISSIONERS
DEC 18 2025
COM _____

SECRETARY'S CERTIFICATE OF

AXON ENTERPRISE, INC.

October 8, 2025

The undersigned certifies that he is the duly elected and qualified Secretary of Axon Enterprise, Inc. ("Axon") and does hereby certify, solely in such capacity and not in an individual capacity, that annexed hereto as Attachment A is a true and correct copy of Axon's list of authorized signatories ("Signature Authority List") as of the date of this certificate.

IN WITNESS WHEREOF, I have signed this certificate as of the date set forth above as the duly elected and qualified Secretary of the Company:

AXON ENTERPRISE, INC.

By: Signed by: Isaiah Fields D415764CFA3141D...

Isaiah Fields
Chief Legal Officer and Corporate Secretary

Attachment:
A – Signature Authority List

ATTACHMENT A

SIGNATURE AUTHORITY LIST – AXON ENTERPRISE, INC.

Abi Stock	Axon Enterprise, Inc.
Alex Engel	Axon Enterprise, Inc.
Amy Nguyen	Axon Enterprise, Inc.
Anas Hammouri	Axon Enterprise, Inc.
Andy Wrenn	Axon Enterprise, Inc.
Angelo Welihindha	Axon Enterprise, Inc.
Ben Hagen	Axon Enterprise, Inc.
Branden Cristello	Axon Enterprise, Inc.
Brandon Rasmussen	Axon Enterprise, Inc.
Brian Fairbanks	Axon Enterprise, Inc.
Brittany Bagley	Axon Enterprise, Inc.
Bryan Wheeler	Axon Enterprise, Inc.
Cameron Brooks	Axon Enterprise, Inc.
Charlie Henick	Axon Enterprise, Inc.
Chris Lindenau	Axon Enterprise, Inc.
Christopher Kirby	Axon Enterprise, Inc.
Clare Manning	Axon Enterprise, Inc.
Craig Trudgeon	Axon Enterprise, Inc.
Dave Beck	Axon Enterprise, Inc.
Dave Iacovelli	Axon Enterprise, Inc.
David Fiorillo	Axon Enterprise, Inc.
Elizabeth Hart	Axon Enterprise, Inc.
Eric Hertz	Axon Enterprise, Inc.
Erik Lapinski	Axon Enterprise, Inc.
Gabrielle Mellon	Axon Enterprise, Inc.
Greg Hewes	Axon Enterprise, Inc.
Hans Moritz	Axon Enterprise, Inc.
Henrik Kühl	Axon Enterprise, Inc.
Hoang Bao	Axon Enterprise, Inc.
Isaiah Fields	Axon Enterprise, Inc.
James Barker	Axon Enterprise, Inc.
James Zito	Axon Enterprise, Inc.
Jay Bennette	Axon Enterprise, Inc.
Jeffrey Kunins	Axon Enterprise, Inc.
Jeffrey Schmidt	Axon Enterprise, Inc.
Jenner Holden	Axon Enterprise, Inc.
Jennifer Mak	Axon Enterprise, Inc.
Jessica Duncan	Axon Enterprise, Inc.
John Henault	Axon Enterprise, Inc.

Joshua Goldman	Axon Enterprise, Inc.
Joshua Isner	Axon Enterprise, Inc.
Karl Schultz	Axon Enterprise, Inc.
Kimberly Murdoch	Axon Enterprise, Inc.
Mark VanAntwerp	Axon Enterprise, Inc.
Mark Wachtmann	Axon Enterprise, Inc.
Marin Lersch	Axon Enterprise, Inc.
Matt Haynes	Axon Enterprise, Inc.
Maura Ballantyne	Axon Enterprise, Inc.
Meredith Sharpe	Axon Enterprise, Inc.
Mike Shore	Axon Enterprise, Inc.
Mike Wagers	Axon Enterprise, Inc.
Nache Shekarri	Axon Enterprise, Inc.
Nathan Sawtell	Axon Enterprise, Inc.
Nick Stamas	Axon Enterprise, Inc.
Pam Petersen	Axon Enterprise, Inc.
Patrick Madden	Axon Enterprise, Inc.
Patrick Smith	Axon Enterprise, Inc.
Paul Strozier	Axon Enterprise, Inc.
Rachel Scott	Axon Enterprise, Inc.
Ran Mokady	Axon Enterprise, Inc.
Robert E. Driscoll Jr.	Axon Enterprise, Inc.
Robert Murphy	Axon Enterprise, Inc.
Sumegh Sodani	Axon Enterprise, Inc.
Thi Luu	Axon Enterprise, Inc.
Tony Biaggne	Axon Enterprise, Inc.
Tracy Stone	Axon Enterprise, Inc.
Vanessa Alexander	Axon Enterprise, Inc.
Vanessa Wirth Bremer	Axon Enterprise, Inc.
Vishal Dhir	Axon Enterprise, Inc.
Vito Sabella	Axon Enterprise, Inc.
Will Steenken	Axon Enterprise, Inc.
Yasser Ibrahim	Axon Enterprise, Inc.

Address and phone number for Officers and Directors:
c/o Axon Enterprise, Inc.
17800 N. 85th Street
Scottsdale, Arizona 85255
1-800-978-2737

Contract No. 2526-10211
Description: Digital Evidence Management System

Attachment 1Reference Agency Name: UNIVERSITY OF NEBRASKA MASTER AGREEMENT #3544-21-4615

UNIVERSITY OF NEBRASKA

MASTER AGREEMENT #3544-21-4615

for

Body Worn Cameras and Related Products and Services

with

Axon Enterprise, Inc.

Effective: December 21, 2022

The following documents comprise the executed contract between The University of Nebraska and Axon Enterprise, Inc., effective December 21, 2022:

I. Master Agreement
II. The University of Nebraska – RFP #3544-21-4615, incorporated by reference
III. Supplier's Response to the RFP, incorporated by reference

UNIVERSITY OF NEBRASKA
MASTER AGREEMENT
3544-21-4615

This Master Agreement (the "Agreement") sets forth the terms between The Board of Regents of the University of Nebraska a public body corporate and governing body of the University of Nebraska for and on behalf of the University of Nebraska Medical Center,having an address at 3835 Holdrege Street, Lincoln, NE 68583 (the "University") and Axon Enterprise, Inc., having anaddress at17800 N. 85th Street, Scottsdale, Arizona 85255 (the "Service Provider") with regard to the performance by Service Provider of the services contemplated herein.

RECITALS

WHEREAS, the University desires to obtain the services of the Service Provider; and

WHEREAS, the Service Provider claims to have expertise and experience to provide such services for the University;

THEREFORE, the University and the Service Provider hereby agree to the following terms, obligations and conditions
:

1. Description of Services. The Service Provider agrees to perform such professional services, with the standard of professional care and skill customarily provided in the performance of such services, and shall use its best efforts to render the services and provide the deliverables identified in an attached proposal and/or scope of work for each engagement which references this Agreement, and in accordance with the supplemental terms attached hereto as Attachment A and Appendix A. The Service Provider agrees to perform the Services to the satisfaction of the University during the term of this Agreement. The attachments, appendices, addendums, any exhibits and schedules hereto are an integral part of this Agreement and are deemed incorporated by reference herein.

2. Payment. In full consideration for the Services performed by the Service Provider under this Agreement, the University shall pay or cause to be paidto the Service Provider the total fee and any incidentals pursuant to the schedule identified in attached documents, including but not limited to quotes and order forms, to this Agreement, attached hereto and incorporated by reference herein, and upon submissionof an invoice to University by the Service Provider. Any additional incidental or reimbursable expenses not described in Exhibit A must be agreed to in writing by an authorized University representative. Along with its invoice, the Service Provider shall submit adequate receipts and documentation as requested by the University to support reimbursement of all previously agreed upon incidental or reimbursable expenses. Service Provider is expected to comply with applicable policies and procedures, including but not limited to those stated within the University of Nebraska TravelPolicy (accessible at https://nebraska.edu/-/media/unca/docs/offices-and-policies/policies/policies/university-of-nebraska-travel-policy.pdf). The University, in its sole discretion, may decline to reimburse incidental or reimbursable expenses that fail to comply with applicable policies andprocedures. All payments due to Service Provider shall be made on a net 30 day basis. The Service Provideragrees that it is solely responsible for payment of income, social security, and other employment taxes due to the proper taxing authorities, and that the University will not deduct such taxes f rom any payments to the Service Provider hereunder, unless required by law.

3. Term. The term of this Agreement shall begin on the date fully executed and remain in place for five (5) year(s). The contract may be renewed, by mutual agreement of both parties, in writing for three (3) additional one (1) year periods upon completion of the initial base contract period, provided written mutual concurrence of both parties is exercised in writing prior to the expiration of the existing contract. The length of the contract in its entirety will not exceed eight (8) years ("Term"). The University of Nebraska reserves the right to contract certain work as needed to provide emergency or timely services, introduction of new technology and/or as a result of general market conditions.

4. Confidentiality. "Confidential Information" shall mean any materials, written information, and data marked "Confidential" by the University, non-written information and data disclosed by the University that is identified at the time of disclosure to the Service Provider as confidential and is reduced to writing and transmitted to the Service Provider within thirty (30) days of such non-written disclosure, or information that, given the nature of the information or circumstances surrounding disclosure, should reasonably be understood to be confidential. The Service Provider agrees to use the same degree of care it usesto protect its own confidential information

and, to the extent permitted by law, to maintain the Confidential Information in strict confidence for a period of three (3)years from the date of termination of this Agreement. The obligations of this paragraph do not apply to information in the public domain or information that is independently known, obtained or discovered by the Service Provider, or that is hereafter supplied to the Service Provider by a third party without restriction.

5. Ownership Intellectual Property Rights. Service Provider owns and reserves all right, title, and interest in goods and services and suggestions to Service Provider, including all related intellectual property rights. The University will not intentionally cause any Service Provider proprietary rights to be violated.

6. Termination. In the event that either party commitsa material breach of this Agreement and fails to remedyor cure such breach within thirty (30) days after receipt of written notice thereof from the non-breaching party, the non-breaching party may, at its option and in addition to any other remedies which it may have at lawor in equity, terminate this Agreement by sending written notice of termination to the other party. Such termination shall be effective as of the date of its receipt. Additionally, the University may terminate this Agreement for its convenience upon thirty (30) days prior written notice to the Service Provider. Upon any termination, the University shall promptly pay the Service Provider for all services rendered and costs incurred up to and including the effective date of termination or Service Provider will refund to University a prorated share of any prepaid fees.

7. Representations and Warranties. The Service Provider represents and warrants that in performing the Services it will not be in breach of any agreement with a third party. The Service Provider agrees to hold University and its respective assigns andlicensees harmless from any loss, damage or expense, including court costs and reasonable attorneys' fees, that University and its assigns and licensees may suffer as a result of a breach or alleged breach of the foregoing warranties or as a result of claims or actions of any kind or nature resulting from the provision of theServices or any infringement of any United States patent, copyright, trade infringement, or other intellectual property right arising out of the manufacturer, delivery and use of any goods or Services by the University. Services Provider's indemnification obligations within this paragraph do not extend to claims do not apply to claims based on (a) modification of the goods or services by the University or a third party not approved by Service Provider; (b) use of the goods or services in combination with hardware or services not approved by Service Provider; (c) use of goods or services in a manner other than as permitted in this Agreement; or (d) use of infringing software that is not the most current release provided by Service Provider.

Each party warrants and represents that it has full power and authority to enter into and perform this Agreement, and that the person signing this Agreementon behalf of each party has been properly authorized and empowered to enter into this Agreement.

8. Independent Service Provider. The Service Provider is an independent Service Provider and is solely responsible for maintenance and payment of anyand all taxes, insurances and the like that may be required by federal, state or local law with respect to any sums paid hereunder. The Service Provider is not the University's agent or representative and has no authority to bind or commit the University to any agreements or other obligations.

9. Liability. Service Provider agrees to indemnify andhold the University, its regents, officers, employees, agents and students, harmless from any loss, claim, damage or liability of any kind brought by a third party, to the extent arising out of or in connection with the negligent or willfully wrongful performance of the Services by theService Provider.

10. Insurance. The Service Provider shall at its own expense obtain and maintain throughout the term of this Agreement general commercial liability insurance against claims for bodily injury, death and property damage with limits of not less than one million dollars ($1,000,000) per occurrence, and three million dollars ($3,000,000) general aggregate, naming The Board of Regents of the University of Nebraska as an additionalinsured, to cover such liability caused by, or arising out of, activities of the Service Provider and its agents and/or employees while engaged in or preparing for theprovision of the Services. The Service Provider shall furnish to the University certificates of insurance evidencing that such insurance has been procured priorto commencement of such work.

11. Assignment. This Agreement is non-assignableand non-transferrable. Any attempt by either party to assign its obligations hereunder shall be void. The foregoing restriction on assignment shall not apply to a transfer to any of Service Provider's affiliates or to any successor corporation as the result of a merger, acquisition or internal reorganization.

12. Amendment. This Agreement constitutes the entire understanding between the Service Provider and the University with respect to the subject matter hereofand may not be amended except by an agreement signed by the Service Provider and an authorized representative of the University.

13. Governing Law and Forum. This Agreement shallbe governed by the laws of the State of Nebraska without giving effect to its conflicts of laws provisions. Any legal actions brought by either party hereunder shall be in the District Court of Lancaster County, Nebraska.

14. Conflict of Interest. No article or service shall be

purchased f rom any University faculty or staff member without prior approval by the Vice Chancellor of Business and Finance and any such approved purchase shall comply fully with the requirements of theconflict of interest provisions of the Nebraska Political Accountability and Disclosure Act, Neb. Rev. Stat., §§ 49-1493 through 49-14,104.

Service Provider certifies, to the best of its knowledge and belief, that there are no potential organizational conflicts of interest related to this Agreement. If ServiceProvider cannot so certify, it shall provide a disclosure statement to the University, which describes all relevantinformation concerning any potential conflict of interest under this Agreement. In the event the potential conflictof interest cannot be resolved, the University may declare this Agreement void and of no further force or effect and the University shall have no further obligations hereunder.

15. Personal Use Prohibited. University funds shallnot be expended for articles or services which are for the personal use of staff or faculty members.

16. Work Status Verification. The Service Provider and its subcontractors shall use a federal immigration verification system to determine the work eligibility status of new employees physically performing serviceswithin the State of Nebraska pursuant to Neb. Rev. Stat. §§ 4-108 to 4-114 as amended.

17. Debarment List. No contract shall be awarded to any Service Provider/Bidder listed on the General Services Administration's List of Parties Excluded f rom Federal Procurement or Nonprocurement Programs in accordance with Executive Orders 12549 and 12689, "Debarment and Suspension," (the "Debarment List"). For contracts which in the aggregate exceed $25,000, Service Provider/Bidder specifically warrants and represents that it is not included on the Debarment List. Service Provider/Bidder further agrees that should it be included on the Debarment List at the time the contract/proposal is awarded, or at any time during which it performs its contractual obligations pursuant to the contract, such listing shall be considered a material breach of the contract between the University and the Service Provider.

18. Change Proposals. Material changes in scope, rush delivery, rework of items already approved or requests for additional revision cycles, services and/or deliverables beyond those listed herein hereafter knownas change orders, shall not be effective until authorized representatives of both Parties execute a mutually acceptable written change order to this Agreement. Any fees arising from change orders, additional services, or deliverables not reflected herein will be invoiced upon completion. Change orders agreed to byemail shall be valid and enforceable as if made part of this Agreement.

19. Taxpayer Transparency Act. Pursuant to Nebraska's Taxpayer Transparency Act (Neb. Rev. Stat. §84-602.01, as may be amended), as of July 1, 2014, the University of Nebraska is required to provide the Nebraska Department of Administrative Services with a copy of each contract that is a basis for an expenditure of state funds, including any documents incorporated by reference in the contract. Copies of all such contracts and documents are published by the Nebraska Department of Administrative Services at www.nebraskaspending.gov. It shall be the sole responsibility of the Service Provider to notify the University of any redactions to such contracts and documents under Neb. Rev. Stat. 84-712.05(3) prior to contract execution. In addition, Supplier agrees to defend any challenge to such redactions at its own expense.

20. Equal Opportunity. This Service Provider and subcontractors shall abide by the requirements of 41 CFR 60-1.4(a), 60-300.5(a) and 60-741.5(a). These regulations prohibit discrimination against qualified individuals based on their status as protected veterans or individuals with disabilities, and prohibit discrimination against all individuals basedon their race, color, religion, sex, sexual orientation, gender identity or national origin. Moreover, these regulations require that covered Service Providers and subcontractors take affirmative action to employ and advance in employment individuals without regard to race, color, religion, sex, sexual orientation, gender identity, national origin, disability or veteran status.

21. Nondiscrimination. In accordance with the Nebraska Fair Employment Practice Act, Neb. Rev. Stat. §48-1122, Service Provider agrees that neither itnor any of its subcontractors shall discriminate againstany employee, or applicant for employment to be employed in the performance of this Agreement, with respect to hire, tenure, terms, conditions or privilege ofemployment because of the race, color, religion, sex, disability, or national origin of the employee orapplicant.

22. Logos or University Marks. The Service Provider shall not use or display any University campus name, logo, trademark, service mark (individually a "Mark" and collectively the "Marks") and/or other indicia designatedby the University as a source identifier, unless expressly authorized in writing by the University. Any unauthorized use of University Marks is expressly prohibited.

23. Right to Audit Privilege. The University reservesthe right to audit or inspect work performed by the Service Provider under this Agreement. The Universitymay participate directly or through an appointed representative, e.g. external auditor, in order to verify that the Services related to this Agreement have been performed in accordance to the

procedures indicated.

24. Continuation of Services. Service Provider agreesto continue to honor its ongoing obligations under this Agreement without interruption in the event of a bonafide dispute concerning payment or a dispute concerning any provision of this Agreement which may include time spent negotiating renewals.

25. Purchase Order Requirement. A Purchase Ordershall be issued by the University to the Service Providerfor payment in accordance with the terms of this Agreement. All invoice(s) submitted by the Service Provider shall make reference to the appropriate Purchase Order number to be eligible for payment.

26. Compliance. Service Provider will comply with all applicable laws, rules, regulations, ordinances and University policies in providing the Services.

27. Incorporation and Priority of Documents. Each document that is ancillary to this Agreement (including without limitation any solicitation, purchase order, addendum, exhibit, appendix, bid, proposal, quotation, or statement of work) ("Ancillary Document") constitutes part of this Agreement if the Ancillary Document is signed by an authorized signatory from each party. Notwithstanding the foregoing, any Ancillary Document attached to the Agreement at execution constitutes part of this Agreement without execution of the Ancillary Document by the parties.

Notwithstanding any provision to the contrary in any of the following documents, precedence is established by the order of the following documents: 1) duly executed amendments to this Agreement (to the extent not superseded by a subsequent amendment); 2) this Agreement and any solicitation, purchase order, addendum, exhibit, attachment, or appendix issued by the University and incorporated by reference into this Agreement; and 3) each bid, proposal, quotation, statement of work, or other Ancillary Document incorporated by reference into this Agreement. In the event of conflicting or inconsistent provisions between any of the foregoing documents, a document identified with a lower numerical value in this section shall supersede a document identified with a higher numerical value in this section to the extent necessary to resolve any such conflict or inconsistency. Provided, however, that in the event an issue is addressed in one of the foregoing documents but is not addressed in another of such documents, no conflict or inconsistency shall be deemed to occur. Where terms and conditions specified in the Service Provider's bid, proposal, or quotation differ from the terms and conditions in University's solicitation, the terms and conditions in the solicitation shall apply. Where terms and conditions specified in the Service Provider's bid, proposal, or quotation supplement the terms and conditions in University's solicitation, the supplemental terms and conditions shall apply only if specifically accepted by University in writing.

The rest of this page is left intentionally blank.

The Board of Regents of the University of Nebraska (the University)

Signature: Chris Kabourek **Date:** 12/21/22 | 12:48 CST

Printed Name: Chris Kabourek

Title: Senior VP | CFO

Full Legal Name of Undersigned (the Undersigned) Axon Enterprise, Inc.

Signature: Robert E Driscoll **Date:** 12/16/2022 | 12:06 PM MST

55DAEBB131A4424...

Printed Name: Robert E Driscoll

Title: VP, Assoc. General Counsel

I affirm that if I am an employee of the University of Nebraska, I have notified buyer of my status as such and that this contract must be completed in accordance with Board of Regents Policy 6.2.1.12, Purchases Involving University Personnel.

With copies provided to:
University Procurement Services
ATTN: Contract Administration
1700 Y Street
Lincoln, NE 68588

Notice. Any notice to either party hereunder shall be in writing and shall be served either personally or by registered or certified mail addressed to the following individuals:

To the Service Provider:

Axon Enterprise, Inc.
17800 N 85th Street
Scottsdale, AZ 85255
Attn: General Counsel

To the University:

Legal Notices
C/O P2P Procurement Contracts
1700 Y Street, BSC 125
Lincoln, NE 68588-0645

Attachment A to University of Nebraska Master Agreement

This Master Services and Purchasing Agreement ("**Agreement**") is between Axon Enterprise, Inc., a Delaware corporation ("**Axon**"), and the Board of Regents of the University of Nebraska ("**Agency**"). This Agreement is effective as of the later of the (a) last signature date on this Agreement or (b) signature date on the Quote ("**Effective Date**"). Axon and Agency are each a "**Party**" and collectively "**Parties**". This Agreement governs Agency's purchase and use of the Axon Devices and Services detailed in the Quote Appendix ("**Quote**"). It is the intent of the Parties that this Agreement, together with the University of Nebraska Master Agreement ("Master Agreement") to which it is attached, act as a master agreement governing all subsequent purchases by Agency for the same Axon products and services in the Quote, and all such subsequent quotes accepted by Agency shall be also incorporated into this Agreement by reference as a Quote. The Parties therefore agree as follows:

1 **Definitions**.

"Agency Content" has the meaning given in Axon Cloud Services Terms of Use Appendix. Axon recognizes and agrees that Agency Content may contain Personal Data, even if the presence of such data is not disclosed and even if such data is not labeled or otherwise identified.

"**Axon Cloud Services**" means Axon's web services for Axon Evidence, Axon Records, Axon Dispatch, and interactions between Evidence.com and Axon Devices or Axon client software. Axon Cloud Service excludes third-party applications, hardware warranties, and my.evidence.com.

"**Axon Device**" means all hardware provided by Axon under this Agreement.

"Personal Data" has the meaning given in Axon Cloud Services Terms of Use Appendix.

"**Non-Content Data**" has the meaning given in Axon Cloud Services Terms of Use Appendix.

"**Quote**" means an offer to sell and is only valid for devices and services on the quote at the specified prices. Any terms within Agency'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 offer by Axon, and Axon reserves the right to cancel any orders resulting from such errors.
"**Services**" means all services provided by Axon under this Agreement, including software, Axon Cloud Services, and professional services.

2 **Term and Survival**. This Term of the Master Agreement shall be as detailed therein ("**Term**").

All subscriptions purchased under this Agreement including Axon Evidence, Axon Fleet, Officer Safety Plans, Technology Assurance Plans, and TASER 7 plans begin upon the date specified in the relevant Quote. Each subscription term ends upon completion of the subscription stated in the Quote ("**Subscription Term**"). If a subscription has not yet expired or been terminated at the end of the Term of the Master Agreement (as may have been extended), such subscription does not terminate and will continue to be governed by the terms of the Agreement and Master Agreement until the subscription's expiration or termination.

3 **Payment**. Axon invoices upon shipment. Payment is due net 30 days from the invoice date. Payment obligations are non-cancelable. Agency will pay invoices without setoff, deduction, or withholding. If Axon sends a past due account to collections, Agency is responsible for collection and attorneys' fees.

4 **Taxes**. Agency shall provide Axon a valid tax exemption certificate.

5 **Shipping**. Axon may make partial shipments and ship Axon Devices from multiple locations. All shipments are FOB shipping point via common carrier. Title and risk of loss pass to Agency upon Axon's delivery to the common carrier. Agency is responsible for any shipping charges in the Quote.

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

7 **Warranty**.

7.1 **Hardware Limited Warranty**. Axon warrants that Axon-manufactured Devices are free from defects in workmanship and materials for 1 year from the date of Agency's receipt, except Signal Sidearm, which Axon warrants for 30 months from the date of Agency's receipt. Axon warrants its Axon-manufactured accessories for 90-days from the date of Agency's receipt. Used conducted energy weapon ("**CEW**") cartridges are deemed to have operated properly. Extended warranties run from the expiration of the 1-year hardware warranty through the extended warranty term. Non-Axon manufactured Devices are not covered by Axon's warranty. Agency should contact the manufacturer for support of non-Axon manufactured Devices.

7.2 **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 Device with the same or like Device, at Axon's option. A replacement Axon Device will be new or like new. Axon will warrant the replacement Axon Device for the longer of (a) the remaining warranty of the original Axon Device or (b) 90-days from the date of repair or replacement.

If Agency exchanges a device or part, the replacement item becomes Agency's property, and the replaced item becomes Axon's property. Before delivering a Axon Device for service, Agency must upload Axon 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 Device sent to Axon for service.

7.3 **Spare Axon Devices**. For qualified purchases, Axon may provide Agency 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 Agency 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 Agency in accordance with shipping terms under Section 5. Axon assumes no liability or obligation in the event Agency does not utilize Spare Axon Devices for the intended purpose.

7.4 **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.

7.4.1 **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.**

7.4.2 **Except to the extent such limitations are prohibited by applicable law, Axon's cumulative liability to any Party for any loss or damage resulting from any claim, demand, or action arising out of or relating to any Axon Device or Service will not exceed $500,000.00. Neither Party will be liable for special, indirect, incidental, punitive or consequential damages, however caused, whether for breach of warranty or contract, negligence, strict liability, tort or any other legal theory**.

8 **Statement of Work**. Certain Axon Devices and Services, including Axon Interview Room, Axon Channel Services, and Axon Fleet, may require a Statement of Work that details Axon's Service deliverables ("**SOW**"). In the event Axon provides an SOW to Agency, Axon is only responsible to perform Services described in the SOW. Additional services 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. The 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 changes to any Axon Device or Service without notifying Agency or making the same change to Axon Devices and Services previously purchased by Agency, provided that it does not materially derogate the overall quality of the Services. Axon will notify the Agency of design

change, at the same time it notifies its general customer base, in the event such design change is in response to a known product defect.

11 **Bundled Offerings**. Some offerings in bundled offerings may not be generally available at the time of Agency's purchase. Axon will not provide a refund, credit, or additional discount beyond what is in the Quote due to a delay of availability or Agency's election not to utilize any portion of an Axon bundle.

12 **Insurance**. Axon will maintain General Liability, Workers' Compensation, and Automobile Liability insurance. Upon request, Axon will supply certificates of insurance, as described in the Master Agreement.

13 **Indemnification**. Axon will indemnify Agency, Agency's officers, directors, and employees ("**Agency Indemnitees**") against all claims, demands, losses, and reasonable expenses arising out of a third-party claim against an Agency Indemnitee resulting from any negligent act, error or omission, or willful misconduct by Axon under this Agreement, except to the extent of Agency's negligence or willful misconduct, or claims under workers compensation.

14 **IP Rights**. Axon owns and reserves all right, title, and interest in Axon devices and services and suggestions to Axon, including all related intellectual property rights. Agency will not cause any Axon proprietary rights to be violated.

15 **IP Indemnification**. Axon will indemnify Agency Indemnitees against all claims, losses, and reasonable expenses from any third-party claim alleging that the use of Axon Devices or Services infringes or misappropriates the third-party's intellectual property rights (an "Indemnifiable Claim"). Agency must promptly provide Axon with written notice of such claim, tender to Axon the defense or settlement of such claim at Axon's expense and cooperate fully with Axon in the defense or settlement of such claim. Axon's IP indemnification obligations do not apply to claims based on (a) modification of Axon Devices or Services by Agency or a third-party not approved by Axon; (b) use of Axon Devices and Services in combination with hardware or services not approved by Axon; (c) use of Axon Devices and Services other than as permitted in this Agreement; or (d) use of Axon software that is not the most current release provided by Axon.

In case of any indemnifiable claim under Section 15, Axon shall, at its own option, promptly:

15.1 Secure for Agency the right to continue using the Services;

15.2 Replace or modify the Services to make it non-infringing, provided such modification or replacement does not materially degrade any functionality listed in the functional and technical specifications set forth in this Agreement of the documentation for the Services; or

15.3 If such remedies are not commercially practical in Axon's reasonable opinion, refund the fee paid for the Services for every month remaining in the term of the Agreement following the date after which Agency ceases using the Services.

If Axon exercises its rights pursuant to subsection 15.3, Agency shall promptly cease all use of the Services.

16 **Agency Responsibilities**. Agency is responsible for (a) Agency's use of Axon Devices (b) breach of this Agreement or violation of applicable law by Agency or an Agency end user; and (c) a dispute between Agency and a third-party over Agency's use of Axon Devices, except for Indemnifiable Claims under Section 15.

17 **Termination**.

17.1 **For Breach**. A Party may terminate this Agreement for cause if it provides 30 days written notice of the breach to the other Party, and the breach remains uncured at the end of 30 days. If Agency terminates this Agreement due to Axon's uncured breach, Axon will refund prepaid amounts on a prorated basis based on the effective date of termination.

17.2 **By Agency**. If sufficient funds are not appropriated or otherwise legally available to pay the fees, Agency may terminate this Agreement. Agency will deliver notice of termination under this section

as soon as reasonably practicable.

17.3 **Effect of Termination**. Upon termination of this Agreement, Agency rights immediately terminate. Agency remains responsible for all fees incurred before the effective date of termination. If Agency 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 Agency the difference between the MSRP for Axon Devices received, including any Spare Axon Devices, and amounts paid towards those Axon Devices. Only if terminating for non-appropriation, Agency may return Axon Devices to Axon within 30 days of termination. MSRP is the standalone price of the individual Axon Device at the time of sale. For bundled Axon Devices, MSRP is the standalone price of all individual components.

18 **Confidentiality**. "**Confidential Information**" means information designated as confidential or, given the nature of the information or circumstances surrounding disclosure, should reasonably be understood to be confidential. Each Party will take reasonable measures to avoid disclosure, dissemination, or unauthorized use of the other Party's Confidential Information. Unless required by law, neither Party will disclose the other Party's Confidential Information during the Term and for 1-year thereafter. If Agency receives a public records request to disclose Axon Confidential Information, to the extent allowed by law, Agency will provide notice to Axon before disclosure. Such disclosure shall not be a violation of this Section 18. Axon may publicly announce information related to this Agreement.

19 **Use and Disclosure of Agency Content**. Axon may access and use Agency Content solely as necessary to provide the Services to Agency, and unless it receives Agency's prior written consent, Axon: (1) shall not access or use Agency Data for any purpose other than to provide the Services, consistent with its Cloud Services Privacy Policy attached hereto; and (2) shall not give any third-party access to Agency Data, except subcontractors subject to section 26 and Axon's Cloud Services Privacy Policy attached hereto.

20 **Injunction and Enforcement**. Axon agrees that: (1) no adequate remedy exists at law if it fails to perform or breaches any of its obligations in this Agreement; (2) it would be difficult to determine the damages resulting from its breach of this Agreement, and such breach would cause irreparable harm to Agency; and (3) a grant of injunctive relief provides the best remedy for any such breach, without any requirement that Agency prove actual damage or post a bond or other security. Axon waives any opposition to such injunctive relief or any right to such proof, bond, or other security. Axon's obligations in this Agreement (without limitation) apply likewise to Axon's successors, including without limitation to any trustee in bankruptcy. (This section does not limit either party's right to injunctive relief from breaches not listed.)

21 **Privacy and Security Law Compliance**. Axon shall comply with all applicable laws and regulations, governing Axon's access to, use of, and handling of Agency Content.

22 **Approved Region and Data Centers**. Axon shall not transfer Agency Content (or allow its subcontractors to transfer Agency Content) outside the United States unless it receives Agency's prior written consent.

23 **Agency Access**. Agency may access and copy any Agency Content in Axon's possession at any time. Axon shall reasonably facilitate such access and copying promptly after Agency's request, provided Axon may charge its reasonable then-standard fees for any such access and copying or for any related deconversion of data.

24 **Deletion**. Except as set forth in this Agreement, Axon shall not erase Agency Content or any copy thereof without Agency's prior written consent. Further, Axon shall: (1) halt Agency Content deletion promptly if Agency informs Axon that any Agency Content is subject to electronic discovery or otherwise relevant to potential litigation; and (2) at such times as Agency may request (including without limitation as a result of Consumer Requests made mandatory by applicable law), promptly erase all Agency Content from all systems under Axon's control and direct and ensure erasure by any and all of its subcontractors that have access to Agency Content. In erasing Agency Content as required by the Agreement, Axon shall leave no data readable, decipherable, or recoverable on its computers or other media or those of its subcontractors, using the best erasure methods commercially feasible. Upon request after any erasure of Agency Content or any part of it, Axon shall certify such erasure to Agency in writing.

25 **General Security.** Without limiting the generality of its obligations elsewhere in this Agreement, Axon shall exercise commercially reasonable efforts to prevent unauthorized exposure or disclosure of Agency Content.

26 **Employees and Subcontractors.** Axon shall not permit any of its employees, subcontractors, or subcontractor employees to access Agency Content except to the extent that such individual or company needs access to facilitate the Services and is subject to a reasonable written agreement with Axon, or in case of employees, a reasonable written employment policy protecting such data, with terms consistent with those of this Agreement.

27 **Audits**. Axon shall retain a certified public accounting firm to perform an annual audit of the data protection features of the Services and to provide a SOC 2 Type II report, pursuant to the then-current standards of the American Institute of Certified Public Accountants (the "AICPA"). If the AICPA revises its relevant reporting standards, Axon shall retain such accounting firm to provide the report that then most resembles a SOC 2 Type II report. In addition, Axon shall annually conduct its own internal security audit and address security gaps. Axon shall give Agency a copy of the most current report from each audit listed above upon request.

28 **Audit and Test Results**. Any report or other result generated through the tests or audits required by section 27 of this Agreement will be Axon's Confidential Information pursuant to section 18 of this Agreement. If any audit or test referenced above uncovers deficiencies or identifies suggested changes in Axon's provision of the Services, Axon shall exercise reasonable efforts promptly to address such deficiencies and changes, including without limitation by revising the information security program described in section 4 of the Axon Cloud Services Terms of Use Appendix.

29 **Data Incidents**. Axon shall implement and maintain a program for managing unauthorized disclosure of, access to, or use of Agency Content (a "Data Incident"). In case of a Data Incident, or if Axon suspects a Data Incident, Axon shall: (1) promptly, and in any case within forty-eight (48) hours, notify Agency by telephone, in person, or by other real-time, in-person communication; (2) cooperate with Agency and law enforcement agencies, where applicable, to investigate and resolve the Data Incident, including without limitation by providing reasonable assistance to Agency in notifying injured third parties; and (3) otherwise comply with applicable laws governing data breach notification and response, including Neb. Rev. Stat. §§ 87-801 through 87-808. In addition, if the Data Incident results from Axon's breach of the Agreement or negligent or unauthorized act or omission, including without limitation those of its subcontractors or other agents, Axon shall (a) compensate Agency for any reasonable expense related to notification of consumers and (b) provide one (1) year of credit monitoring service to any affected individual. Axon shall give Agency prompt access to such records related to a Data Incident as Agency may reasonably request, and such records will be Axon's Confidential Information pursuant to section 18 (Confidentiality) of this Agreement; provided Axon is not required to give Agency access to records that might compromising the security of Axon's other customers. This section does not limit Agency's other rights or remedies, if any, resulting from a Data Incident.

30 **Services Warranties**. Axon warrants that:

30.1 During the term of this Agreement and subject to Axon's rights to make improvements pursuant to Section 10 of the Agreement, the Services will perform materially as described in the documentation for the Services;

30.2 Axon is the owner of the Services and of each and every component thereof, or the recipient of a valid license thereto;

30.3 Axon has and will maintain the full power and authority to provide the Services described in the Agreement (a) without the further consent of any third party and (b) without conditions or requirements not set forth in the Agreement;

30.4 Axon employs and will employ industry standard or better protections to prevent unauthorized disclosure of or access to personally identifiable information Agency provides to the Services;

30.5 Axon will comply with those laws governing the privacy and security of such information and generally applicable to data processors in the jurisdictions in which Axon does business;

30.6 Axon will perform professional services in a professional and workmanlike manner;

30.7 Axon has the full right and authority to enter into, execute, and perform its obligations under this Agreement and to the best of its knowledge, as of the date of original signature on the Master Agreement, no pending or threatened claim or litigation known to Axon would have a material adverse impact on its ability to perform as required by this Agreement; and

30.8 The Services and any media used to distribute it contain no viruses or other computer instructions or technological means intended to disrupt, damage, or interfere with the use of computers or related systems;

30.9 Axon's performance of the Services will comply with all applicable laws, including without limitation federal, national, state, provincial, and local.

31 **Axon Cloud Services Service Levels**. Axon shall make commercially reasonable efforts to make Axon Cloud Services available 99.99% of the time. In the event that Axon fails to make Axon Cloud Services available to the defined Monthly Uptime Percentage set forth below, Agency may be entitled to Service Credits, which are awarded as days of Axon Cloud Services usage added to the end of the Subscription Term at no charge to Agency, as further set forth in the attached Service Level Agreement.

Monthly Uptime Percentage	Service Credits in Days
Less than 99.9%	3
Less than 99.0%	7

32 **Breach of Professional Services Warranty**. In case of breach of the warranty in subsection 30.6, Axon, at its own expense, shall promptly re-perform the professional services in question. The preceding sentence, in conjunction with Agency's right to terminate the Agreement where applicable, states Agency's sole remedy and Axon's entire liability for breach of the warranty in subsection 30.6.

33 **Third-Party Terms**. Use of software or services other than those provided by Axon is solely governed by the terms, if any, entered into between Agency and the respective third-party provider.

34 **General**.

34.1 **Force Majeure**. Neither Party will be liable for any delay or failure to perform due to a cause beyond a Party's reasonable control.

34.2 **Independent Contractors**. The Parties are independent contractors. Neither Party has the authority to bind the other. This Agreement does not create a partnership, franchise, joint venture, agency, fiduciary, or employment relationship between the Parties.

34.3 **Third-Party Beneficiaries**. There are no third-party beneficiaries under this Agreement.

34.4 **Non-Discrimination**. Neither Party nor its employees will discriminate against any person based on race; religion; creed; color; sex; gender identity and expression; pregnancy; childbirth; breastfeeding; medical conditions related to pregnancy, childbirth, or breastfeeding; sexual orientation; marital status; age; national origin; ancestry; genetic information; disability; veteran status; or any class protected by local, state, or federal law.

34.5 **Export Compliance**. Each Party will comply with all import and export control laws and regulations.

34.6 **Assignment**. Neither Party may assign this Agreement without the other Party's prior written consent. Axon may assign this Agreement, its rights, or obligations without consent: (a) to an affiliate or subsidiary; or (b) for purposes of financing, merger, acquisition, corporate reorganization,

or sale of all or substantially all its assets. This Agreement is binding upon the Parties respective successors and assigns.

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

34.8 **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.

34.9 **Survival**. The following sections will survive termination: Payment, Warranty, Services Warranties, Axon Device Warnings, Indemnification, IP Rights, and Agency Responsibilities.

Governing Law. The laws of the state where Agency is physically located, without reference to conflict of law rules, govern this Agreement and any dispute arising from it.

34.10 **Notices**. All notices must be in English. Notices posted on Agency's Axon Evidence site are effective upon posting. Notices by email are effective on the sent date of the email. Notices by personal delivery are effective immediately. Contact information for notices:

Axon: Axon Enterprise, Inc. Attn: Legal 17800 N. 85th Street Scottsdale, Arizona 85255 legal@axon.com	Agency: Attn: Street Address City, State, Zip Email

34.11 **Entire Agreement**. The Master Agreement, together with this Agreement, including the Appendices and any SOW(s), represents the entire agreement between the Parties. In the event of a conflict between the Master Agreement and this Agreement, the Master Agreement shall take precedence. This Agreement may only be modified or amended in a writing signed by the Parties.

Each representative identified below declares they have been expressly authorized to execute this Agreement as of the date of signature.

Axon Enterprise, Inc.	**Agency**
Signature: DocuSigned by: Robert E Driscoll 55DAEBB131A4424...	Signature: Chris Kabourek
Name: Robert E Driscoll	Name: Chris Kabourek
Title: VP, Assoc. General Counsel	Title: Senior VP | CFO
Date: 12/16/2022 | 12:06 PM MST	Date: 12/21/22 | 12:48 CST

Axon Cloud Services Terms of Use Appendix

1 **Definitions**.
"Agency Content" is data uploaded into, ingested by, or created in Axon Cloud Services within Agency's tenant, including media or multimedia uploaded into Axon Cloud Services by Agency. Agency Content includes Evidence but excludes Non-Content Data.

"**Evidence**" is media or multimedia uploaded into Axon Evidence as 'evidence' by an Agency. Evidence is a subset of Agency Content.

"**Non-Content Data**" is data, configuration, and usage information about Agency'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 Agency Content.

"**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.

2 **Access**. Upon Axon granting Agency a subscription to Axon Cloud Services, Agency may access and use Axon Cloud Services to store and manage Agency Content. Agency may not exceed more end users than the Quote specifies. Axon Air requires an Axon Evidence subscription for each drone operator. For Axon Evidence Lite, Agency may access and use Axon Evidence only to store and manage TASER CEW and TASER CAM data ("**TASER Data**"). Agency may not upload non-TASER Data to Axon Evidence Lite.

3 **Agency Owns Agency Content**. Agency controls and owns all right, title, and interest in Agency Content. Except as outlined herein, Axon obtains no interest in Agency Content, and Agency Content is not Axon's business records. Agency is solely responsible for uploading, sharing, managing, and deleting Agency Content. Axon will only have access to Agency Content for the limited purposes set forth herein. Agency agrees to allow Axon access to Agency 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 Agency Content against accidental or unlawful loss, access or disclosure. Axon will maintain a comprehensive information security program to protect Axon Cloud Services and Agency 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.

5 **Agency Responsibilities**. Agency is responsible for (a) ensuring Agency owns Agency Content; (b) ensuring no Agency Content or Agency end user's use of Agency Content or Axon Cloud Services violates this Agreement or applicable laws; and (c) maintaining necessary computer equipment and Internet connections for use of Axon Cloud Services. If Agency becomes aware of any violation of this Agreement by an end user, Agency will immediately terminate that end user's access to Axon Cloud Services.

Agency will also maintain the security of end user names and passwords and security and access by end users to Agency Content. Agency is responsible for ensuring the configuration and utilization of Axon Cloud Services meet applicable Agency regulation and standards. Agency may not sell, transfer, or sublicense access to any other entity or person. Agency shall contact Axon immediately

if an unauthorized party may be using Agency's account or Agency Content, or if account information is lost or stolen.

To the extent Agency 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**. Agency's use of Axon Cloud Services is subject to the Axon Cloud Services Privacy Policy, which is incorporated by reference into and appended to this Agreement. Agency agrees to allow Axon access to Non-Content Data from Agency 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. Notwithstanding the provisions anything to the contrary in this Agreement, Axon may disclose Agency Content or Non-Content Data as required by applicable law or by proper legal or governmental authority. Axon shall give Agency prompt notice of any such legal or governmental demand and reasonably cooperate with Agency in any effort to seek a protective order or otherwise to contest such required disclosure, at Agency's expense. No revision of Axon's privacy policy will alter Agency's rights and remedies in this Agreement.

7 **Axon Body 3 Wi-Fi Positioning**. Axon Body 3 cameras offer a feature to enhance location services where GPS/GNSS signals may not be available, for instance, within buildings or underground. Agency administrators can manage their choice to use this service within the administrative features of Axon Cloud Services. If Agency chooses to use this service, Axon must also enable the usage of the feature for Agency's Axon Cloud Services tenant. Agency will not see this option with Axon Cloud Services unless Axon has enabled Wi-Fi Positioning for Agency's Axon Cloud Services tenant. When Wi-Fi Positioning is enabled by both Axon and Agency, Non-Content and Personal Data will be sent to Skyhook Holdings, Inc. ("**Skyhook"**) to facilitate the Wi-Fi Positioning functionality. Data controlled by Skyhook is outside the scope of the Axon Cloud Services Privacy Policy and is subject to the Skyhook Services Privacy Policy.

8 **Storage**. For Axon Unlimited Device Storage subscriptions, Agency may store unlimited data in Agency's Axon Evidence account only if data originates from Axon Capture or the applicable Axon Device. Axon may charge Agency additional fees for exceeding purchased storage amounts. Axon may place Agency Content that Agency has not viewed or accessed for 6 months into archival storage. Agency Content in archival storage will not have immediate availability and may take up to 24 hours to access.

9 **Location of Storage**. Axon may transfer Agency Content to third-party subcontractors for storage. Axon will determine the locations of data centers for storage of Agency Content. For United States agencies, Axon will ensure all Agency Content stored in Axon Cloud Services remains within the United States. Ownership of Agency Content remains with Agency.

10 **Suspension**. Axon may temporarily suspend Agency's or any end user's right to access or use any portion or all of Axon Cloud Services immediately upon notice, if Agency 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.

Agency remains responsible for all fees incurred through suspension. Axon will not delete Agency Content because of suspension, except as specified in this Agreement.

11 **Axon Cloud Services Warranty**. Except as set forth in this Agreement, Axon disclaims any warranties or responsibility for data corruption or errors before Agency uploads data to Axon Cloud Services.

12 **Axon Records**. Axon Records is the software-as-a-service product that is generally available at the time Agency purchases an OSP 7 bundle. During Agency's Axon Records Subscription Term, Agency will be entitled to receive Axon's Update and Upgrade releases on an if-and-when available basis.

The Axon Records Subscription Term will end upon the completion of the Axon Records Subscription as documented in the Quote, or if purchased as part of an OSP 7 bundle, upon competition of the OSP 7 Term ("**Axon Records Subscription**")

An "**Update**" is a generally available release of Axon Records that Axon makes available from time to time. An "**Upgrade**" includes (i) new versions of Axon Records that enhance features and functionality, as solely determined by Axon; and/or (ii) new versions of Axon Records that provide additional features or perform additional functions. Upgrades exclude new products that Axon introduces and markets as distinct products or applications.

New or additional Axon products and applications, as well as any Axon professional services needed to configure Axon Records, are not included. If Agency purchases Axon Records as part of a bundled offering, the Axon Record subscription begins on the later of the (1) start date of that bundled offering, or (2) date Axon provisions Axon Records to Agency.

13 **Axon Cloud Services Restrictions**. Agency and Agency end users (including employees, contractors, agents, officers, volunteers, and directors), may not, or may not attempt to:

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

13.2 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;

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

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

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

13.6 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

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

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

15 **Post-Termination Assistance**. Axon will provide Agency 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 Agency 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.

16 **U.S. Government Rights**. If Agency 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 Agency 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, Agency will immediately discontinue use of Axon Cloud Services.

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

Axon Customer Experience Improvement Program Appendix

1 **Axon Customer Experience Improvement Program (ACEIP)**. The ACEIP is designed to accelerate Axon's development of technology, such as building and supporting automated features, to ultimately increase safety within communities and drive efficiency in public safety. To this end, subject to the limitations on Axon as described below, Axon, where allowed by law, may make limited use of Agency Content from all of its customers, to provide, develop, improve, and support current and future Axon products (collectively, "**ACEIP Purposes**"). However, at all times, Axon will comply with its obligations pursuant to the Axon Cloud Services Terms of Use Appendix to maintain a comprehensive data security program (including compliance with the CJIS Security Policy for Criminal Justice Information), privacy program, and data governance policy, including high industry standards of de-identifying Personal Data, to enforce its security and privacy obligations for the ACEIP. ACEIP has 2 tiers of participation, Tier 1 and Tier 2. By default, Agency will be a participant in ACEIP Tier 1. If Agency does not want to participate in ACEIP Tier 1, Agency can revoke its consent at any time. If Agency wants to participate in Tier 2, as detailed below, Agency can check the ACEIP Tier 2 box below. If Agency does not want to participate in ACEIP Tier 2, Agency should leave box unchecked. At any time, Agency may revoke its consent to ACEIP Tier 1, Tier 2, or both Tiers.

1.1 ACEIP Tier 1.

1.1.1. When Axon uses Agency Content for the ACEIP Purposes, Axon will extract from Agency Content and may store separately copies of certain segments or elements of the Agency Content (collectively, "**ACEIP Content**"). When extracting ACEIP Content, Axon will use commercially reasonable efforts to aggregate, transform or de-identify Agency Content so that the extracted ACEIP Content is no longer reasonably capable of being associated with, or could reasonably be linked directly or indirectly to a particular individual ("**Privacy Preserving Technique(s)**"). For illustrative purposes, some examples are described in footnote 1[1]. For clarity, ACEIP Content will still be linked indirectly, with an attribution, to the Agency from which it was extracted. This attribution will be stored separately from the data itself, but is necessary for and will be solely used to enable Axon to identify and delete all ACEIP Content upon Agency request. Once de-identified, ACEIP Content may then be further modified, analyzed, and used to create derivative works. At any time, Agency may revoke the consent granted herein to Axon to access and use Agency Content for ACEIP Purposes. Within 30 days of receiving the Agency's request, Axon will no longer access or use Agency Content for ACEIP Purposes and will delete any and all ACEIP Content. Axon will also delete any derivative works which may reasonably be capable of being associated with, or could reasonably be linked directly or indirectly to Agency. In addition, if Axon uses Agency Content for the ACEIP Purposes, upon request, Axon will make available to Agency a list of the specific type of Agency Content being used to generate ACEIP Content, the purpose of such use, and the retention, privacy preserving extraction technique, and relevant data protection practices

[1] For example; (a) when extracting specific text to improve automated transcription capabilities, text that could be used to directly identify a particular individual would not be extracted, and extracted text would be disassociated from identifying metadata of any speakers, and the extracted text would be split into individual words and aggregated with other data sources (including publicly available data) to remove any reasonable ability to link any specific text directly or indirectly back to a particular individual; (b) when extracting license plate data to improve Automated License Plate Recognition (ALPR) capabilities, individual license plate characters would be extracted and disassociated from each other so a complete plate could not be reconstituted, and all association to other elements of the source video, such as the vehicle, location, time, and the surrounding environment would also be removed; (c) when extracting audio of potential acoustic events (such as glass breaking or gun shots), very short segments (<1 second) of audio that only contains the likely acoustic events would be extracted and all human utterances would be removed.

applicable to the Agency Content or ACEIP Content ("Use Case"). From time to time, Axon may develop and deploy new Use Cases. At least 30 days prior to authorizing the deployment of any new Use Case, Axon will provide Agency notice (by updating the list of Use Case at https://www.axon.com/aceip and providing Agency with a mechanism to obtain notice of that update or another commercially reasonable method to Agency designated contact) ("**New Use Case**").

1.1.2. **Expiration of ACEIP Tier 1**. Agency consent granted herein, will expire upon termination of the Agreement. In accordance with section 1.1.1, within 30 days of receiving the Agency's request, Axon will no longer access or use Agency Content for ACEIP Purposes and will delete ACEIP Content. Axon will also delete any derivative works which may reasonably be capable of being associated with, or could reasonably be linked directly or indirectly to Agency.

1.2 **ACEIP Tier 2**. In addition to ACEIP Tier 1, if Agency wants to help further improve Axon's services, Agency may choose to participate in Tier 2 of the ACEIP. ACEIP Tier 2, grants Axon certain additional rights to use Agency Content, in addition to those set forth in Tier 1 above, without the guaranteed deployment of a Privacy Preserving Technique to enable product development, improvement, and support that cannot be accomplished with aggregated, transformed or de-identified data.

Professional Services Appendix

1 **Utilization of Services**. Agency must use professional services as outlined in the Quote and this Appendix within 6 months of the Effective Date.

2 **Body-Worn Camera Full Service (BWC Full Service)**. BWC Full Service includes advance remote project planning and configuration support and up to 4 consecutive days of on-site service and a professional services manager to work with Agency to assess Agency's deployment and determine which on-site services are appropriate. If Agency requires more than 4 consecutive on-site days, Agency must purchase additional days. BWC Full Service options include:

System set up and configuration • Instructor-led setup of Axon View on smartphones (if applicable) • Configure categories and custom roles based on Agency need • Register cameras to Agency domain • Troubleshoot IT issues with Axon Evidence and Axon Dock ("**Dock**") access • One on-site session included
Dock configuration • Work with Agency to decide the ideal location of Docks and set configurations on Dock • Authenticate Dock with Axon Evidence using admin credentials from Agency • On-site assistance, not to include physical mounting of docks
Best practice implementation planning session • Provide considerations for the establishment of video policy and system operations best practices based on Axon's observations with other agencies • Discuss the importance of entering metadata in the field for organization purposes and other best practice for digital data management • Provide referrals of other agencies using the Axon camera devices and Axon Evidence • Recommend rollout plan based on review of shift schedules
System Admin and troubleshooting training sessions Step-by-step explanation and assistance for Agency's configuration of security, roles & permissions, categories & retention, and other specific settings for Axon Evidence
Axon instructor training (Train the Trainer) Training for Agency's in-house instructors who can support Agency's Axon camera and Axon Evidence training needs after Axon has fulfilled its contractual on-site obligations
Evidence sharing training Tailored workflow instruction for Investigative Units on sharing Cases and Evidence with local prosecuting agencies
End user go-live training and support sessions • Assistance with device set up and configuration • Training on device use, Axon Evidence, and Evidence Sync
Implementation document packet Axon Evidence administrator guides, camera implementation guides, network setup guide, sample policies, and categories & roles guide
Post go-live review

3 **Body-Worn Camera Starter Service (BWC Starter)**. BWC Starter includes advance remote project planning and configuration support and one day of on-site Services and a professional services manager to work closely with Agency to assess Agency's deployment and determine which Services are appropriate. If Agency requires more than 1 day of on-site Services, Agency must purchase additional on-site Services. The BWC Starter options include:

System set up and configuration (Remote Support) • Instructor-led setup of Axon View on smartphones (if applicable) • Configure categories & custom roles based on Agency need • Troubleshoot IT issues with Axon Evidence and Axon Dock ("**Dock**") access
Dock configuration • Work with Agency to decide the ideal location of Dock setup and set configurations on Dock • Authenticate Dock with Axon Evidence using "Administrator" credentials from Agency • Does not include physical mounting of docks
Axon instructor training (Train the Trainer) Training for Agency's in-house instructors who can support Agency's Axon camera and Axon Evidence training needs after Axon's has fulfilled its contracted on-site obligations
End user go-live training and support sessions • Assistance with device set up and configuration • Training on device use, Axon Evidence, and Evidence Sync
Implementation document packet Axon Evidence administrator guides, camera implementation guides, network setup guide, sample policies, and categories & roles guide

4 **Body-Worn Camera Virtual 1-Day Service (BWC Virtual)**. BWC Virtual includes all items in the BWC Starter Service Package, except one day of on-site services.

5 **CEW Services Packages**. CEW Services Packages are detailed below:

System set up and configuration • Configure Axon Evidence categories & custom roles based on Agency need. • Troubleshoot IT issues with Axon Evidence. • Register users and assign roles in Axon Evidence. • **For the CEW Full Service Package**: On-site assistance included • **For the CEW Starter Package**: Virtual assistance included
Dedicated Project Manager Assignment of specific Axon representative for all aspects of planning the rollout (Project Manager). Ideally, Project Manager will be assigned to Agency 4–6 weeks before rollout
Best practice implementation planning session to include: • Provide considerations for the establishment of CEW policy and system operations best practices based on Axon's observations with other agencies • Discuss the importance of entering metadata and best practices for digital data management • Provide referrals to other agencies using TASER CEWs and Axon Evidence • **For the CEW Full Service Package:** On-site assistance included • **For the CEW Starter Package:** Virtual assistance included
System Admin and troubleshooting training sessions On-site sessions providing a step-by-step explanation and assistance for Agency's configuration of security, roles & permissions, categories & retention, and other specific settings for Axon Evidence
Axon Evidence Instructor training • Provide training on the Axon Evidence to educate instructors who can support Agency's subsequent Axon Evidence training needs. • **For the CEW Full Service Package:** Training for up to 3 individuals at Agency • **For the CEW Starter Package:** Training for up to 1 individual at Agency

TASER CEW inspection and device assignment Axon's on-site professional services team will perform functions check on all new TASER CEW Smart weapons and assign them to a user on Axon Evidence.
Post go-live review **For the CEW Full Service Package**: On-site assistance included. **For the CEW Starter Package**: Virtual assistance included.

6 **Smart Weapon Transition Service**. The Smart Weapon Transition Service includes:

Archival of CEW Firing Logs Axon's on-site professional services team will upload CEW firing logs to Axon Evidence from all TASER CEW Smart Weapons that Agency is replacing with newer Smart Weapon models.
Return of Old Weapons Axon's on-site professional service team will ship all old weapons back to Axon's headquarters. Axon will provide Agency with a Certificate of Destruction

*Note: CEW Full Service packages for TASER 7 include Smart Weapon Transition Service instead of 1-Day Device Specific Instructor Course.

7 **Signal Sidearm Installation Service**. If Agency purchases Signal Sidearm Installation Service, Axon will provide one day of on-site Services and one professional services manager and will cover the installation of up 100 Signal Sidearm devices per package purchased. Agency is responsible for providing an appropriate work area and ensuring all holsters that will have Signal Sidearm installed onto them are available on the agreed-upon installation date(s). Installation includes:

Removal of existing connection screws that affix a holster to a holster mount
Proper placement of the Signal Sidearm Mounting Plate between the holster and the mount
Reattachment of the holster to the mount using appropriate screws
Functional testing of Signal Sidearm device

8 **Out of Scope Services**. Axon is only responsible to perform the professional services described in the Quote and this Appendix. Any additional professional services are out of scope. The Parties must document scope changes in a written and signed change order. Changes may require an equitable adjustment in the charges or schedule.

9 **Delivery of Services**. Axon personnel will work Monday through Friday, 8:30 a.m. to 5:30 p.m., except holidays. Axon will perform all on-site tasks over a consecutive timeframe. Axon will not charge Agency travel time by Axon personnel to Agency premises as work hours.

10 **Access Computer Systems to Perform Services**. Agency authorizes Axon to access relevant Agency computers and networks, solely for performing the Services. Axon will work to identify as soon as reasonably practicable resources and information Axon expects to use and will provide an initial itemized list to Agency. Agency is responsible for and assumes the risk of any problems, delays, losses, claims, or expenses resulting from the content, accuracy, completeness, and consistency of all data, materials, and information supplied by Agency.

11 **Site Preparation**. Axon will provide a hardcopy or digital copy of current user documentation for the Axon Devices ("**User Documentation**"). User Documentation will include all required environmental specifications for the professional Services and Axon Devices to operate per the Axon Device User Documentation. Before installation of Axon Devices (whether performed by Agency or Axon), Agency must prepare the location(s) where Axon Devices are to be installed ("**Installation Site**") per the environmental specifications in the Axon Device User Documentation. Following installation, Agency must maintain the Installation Site per the environmental specifications. If Axon modifies Axon Device User Documentation for any Axon Devices under this Agreement, Axon will provide the update to Agency when Axon generally releases it

12 **Acceptance**. When Axon completes professional Services, Axon will present an acceptance form ("**Acceptance Form**") to Agency. Agency will sign the Acceptance Form acknowledging completion. If Agency reasonably believes Axon did not complete the professional Services in substantial conformance with this Agreement, Agency must notify Axon in writing of the specific reasons for rejection within 7 calendar days from delivery of the Acceptance Form. Axon will address the issues and re-present the Acceptance Form for signature. If Axon does not receive the signed Acceptance Form or written notification of reasons for rejection within 7 calendar days of delivery of the Acceptance Form, Axon will deem Agency to have accepted the professional Services.

13 **Agency Network**. For work performed by Axon transiting or making use of Agency's network, Agency is solely responsible for maintenance and functionality of the network. In no event will Axon be liable for loss, damage, or corruption of Agency's network from any cause.

Technology Assurance Plan Appendix

If Technology Assurance Plan ("**TAP**") or a bundle including TAP is on the Quote, this appendix applies.

1 **TAP Warranty**. The TAP warranty is an extended warranty that starts at the end of the 1-year Hardware Limited Warranty.

2 **Officer Safety Plan**. If Agency purchases an Officer Safety Plan ("**OSP**"), Agency will receive the deliverables detailed in the Quote. Agency must accept delivery of the TASER CEW and accessories as soon as available from Axon.

3 **OSP 7 Term**. OSP 7 begins after Axon ships the Axon Body 3 or TASER 7 hardware to Agency. If Axon ships in the first half of the month, OSP 7 starts the 1st of the following month. If Axon ships in the second half of the month, OSP 7 starts the 15th of the following month ("**OSP 7 Term**").

4 **TAP BWC Upgrade**. If Agency has no outstanding payment obligations and purchased TAP, Axon will provide Agency a new Axon body-worn camera ("**BWC Upgrade**") as scheduled in the Quote. If Agency purchased TAP Axon will provide a BWC Upgrade that is the same or like Axon Device, at Axon's option. Axon makes no guarantee the BWC Upgrade will utilize the same accessories or Axon Dock.

5 **TAP Dock Upgrade**. If Agency has no outstanding payment obligations and purchased TAP, Axon will provide Agency a new Axon Dock as scheduled in the Quote ("**Dock Upgrade**"). Accessories associated with any Dock Upgrades are subject to change at Axon discretion. Dock Upgrades will only include a new Axon Dock bay configuration unless a new Axon Dock core is required for BWC compatibility. If Agency originally purchased a single-bay Axon Dock, the Dock Upgrade will be a single-bay Axon Dock model that is the same or like Axon Device, at Axon's option. If Agency originally purchased a multi-bay Axon Dock, the Dock Upgrade will be a multi-bay Axon Dock that is the same or like Axon Device, at Axon's option.

6 **Upgrade Delay**. Axon may ship the BWC and Dock Upgrades as scheduled in the Quote without prior confirmation from Agency unless the Parties agree in writing otherwise at least 90 days in advance. Axon may ship the final BWC and Dock Upgrade as scheduled in the Quote 60 days before the end of the Subscription Term without prior confirmation from Agency.

7 **Upgrade Change**. If Agency wants to change Axon Device models for the offered BWC or Dock Upgrade, Agency must pay the price difference between the MSRP for the offered BWC or Dock Upgrade and the MSRP for the model desired. If the model Agency desires has an MSRP less than the MSRP of the offered BWC Upgrade or Dock Upgrade, Axon will not provide a refund. The MSRP is the MSRP in effect at the time of the upgrade.

8 **Return of Original Axon Device**. Within 30 days of receiving a BWC or Dock Upgrade, Agency must return the original Axon Devices to Axon or destroy the Axon Devices and provide a certificate of destruction to Axon including serial numbers for the destroyed Axon Devices. If Agency does not return or destroy the Axon Devices, Axon will deactivate the serial numbers for the Axon Devices received by Agency.

9 **Termination**. If Agency's payment for TAP, OSP, or Axon Evidence is more than 30 days past due, Axon may terminate TAP or OSP. Once TAP or OSP terminates for any reason:

- **9.1** TAP and OSP coverage terminate as of the date of termination and no refunds will be given.
- **9.2** Axon will not and has no obligation to provide the Upgrade Models.
- **9.3** Agency must make any missed payments due to the termination before Agency may purchase any future TAP or OSP.

TASER 7 Appendix

This TASER 7 Appendix applies to Agency's TASER 7, OSP 7, or OSP 7 Plus purchase from Axon.

1 **Duty Cartridge Replenishment Plan**. If the Quote includes "**Duty Cartridge Replenishment Plan**", Agency must purchase the plan for each CEW user. A CEW user includes officers that use a CEW in the line of duty and those that only use a CEW for training. Agency may not resell cartridges received. Axon will only replace cartridges used in the line of duty.

2 **Training**. If the Quote includes a training voucher, Agency must use the voucher within 1 year of issuance, or the voucher will be void. Axon will issue Agency a voucher annually beginning on the start of the TASER Subscription Term. The voucher has no cash value. Agency cannot exchange it for another device or service. Unless stated in the Quote, the voucher does not include travel expenses and will be Agency's responsibility. If the Quote includes Axon Online Training or Virtual Reality Content Empathy Development for Autism/Schizophrenia (collectively, "**Training Content**"), Agency may access Training Content. Axon will deliver all Training Content electronically.

3 **Extended Warranty**. If the Quote includes an extended warranty, the extended warranty coverage period warranty will be for a 5-year term, which includes the hardware manufacturer's warranty plus the 4-year extended term.

4 **Trade-in**. If the Quote contains a discount on CEW-related line items, including items related to OSP, then that discount may only be applied as a trade-in credit, and Agency must return used hardware and accessories associated with the discount ("**Trade-In Units**") to Axon. Agency must ship batteries via ground shipping. Axon will pay shipping costs of the return. If Axon does not receive Trade-In Units within the timeframe below, Axon will invoice Agency the value of the trade-in credit. Agency may not destroy Trade-In Units and receive a trade-in credit.

Agency Size	Days to Return from Start Date of TASER 7 Subscription
Less than 100 officers	30 days
100 to 499 officers	90 days
500+ officers	180 days

5 **TASER 7 Subscription Term**. The TASER 7 Subscription Term for a standalone TASER 7 purchase begins on shipment of the TASER 7 hardware. The TASER 7 Subscription Term for OSP 7 begins on the OSP 7 Start date.

6 **Access Rights**. Upon Axon granting Agency a TASER 7 Axon Evidence subscription, Agency may access and use Axon Evidence for the storage and management of data from TASER 7 CEW devices during the TASER 7 Subscription Term. Agency may not upload any non-TASER 7 data or any other files to Axon Evidence. Agency may not exceed the number of end users than the Quote specifies.

7 **Privacy.** Axon will not disclose Agency Content or any information about Agency except as compelled by a court or administrative body or required by any law or regulation. Axon will give notice if any disclosure request is received for Agency Content, so Agency may file an objection with the court or administrative body.

8 **Termination**. If payment for TASER 7 is more than 30 days past due, Axon may terminate Agency's TASER 7 plan by notifying Agency. Upon termination for any reason, then as of the date of termination:

8.1 TASER 7 extended warranties and access to Training Content will terminate. No refunds

will be given.

8.2 Axon will invoice Agency the remaining MSRP for TASER 7 products received before termination. If terminating for non-appropriations, Axon will not invoice Agency if Agency returns the CEW, rechargeable battery, holster, dock, core, training suits, and unused cartridges to Axon within 30 days of the date of termination.

8.3 Agency will be responsible for payment of any missed payments due to the termination before being allowed to purchase any future TASER 7 plan.

Axon Auto-Tagging Appendix

1 **Scope.** Axon Auto-Tagging consists of the development of a module to allow Axon Evidence to interact with Agency's Computer-Aided Dispatch ("**CAD**") or Records Management Systems ("**RMS**"). This allows end users to auto-populate Axon video meta-data with a case ID, category, and location-based on data maintained in Agency's CAD or RMS.

2 **Support**. For thirty days after completing Auto-Tagging Services, Axon will provide up to 5 hours of remote support at no additional charge. Axon will provide free support due to a change in Axon Evidence, so long as long as Agency maintains an Axon Evidence and Auto-Tagging subscription. Axon will not provide support if a change is required because Agency changes its CAD or RMS.

3 **Changes**. Axon is only responsible to perform the Services in this Appendix. Any additional Services 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.

4 **Agency Responsibilities**. Axon's performance of Auto-Tagging Services requires Agency to:

4.1 Make available relevant systems, including Agency's current CAD or RMS, for assessment by Axon (including remote access if possible);

4.2 Make required modifications, upgrades or alterations to Agency's hardware, facilities, systems and networks related to Axon's performance of Auto-Tagging Services;

4.3 Provide access to the premises where Axon is performing Auto-Tagging Services, subject to Agency safety and security restrictions, and allow Axon to enter and exit the premises with laptops and materials needed to perform Auto-Tagging Services;

4.4 Provide all infrastructure and software information (TCP/IP addresses, node names, network configuration) necessary for Axon to provide Auto-Tagging Services;

4.5 Promptly install and implement any software updates provided by Axon;

4.6 Ensure that all appropriate data backups are performed;

4.7 Provide assistance, participation, and approvals in testing Auto-Tagging Services;

4.8 Provide Axon with remote access to Agency's Axon Evidence account when required;

4.9 Notify Axon of any network or machine maintenance that may impact the performance of the module at Agency; and

4.10 Ensure reasonable availability of knowledgeable staff and personnel to provide timely, accurate, complete, and up-to-date documentation and information to Axon.

5 **Access to Systems.** Agency authorizes Axon to access Agency's relevant computers, network systems, and CAD or RMS solely for performing Auto-Tagging Services. Axon will work diligently to identify as soon as reasonably practicable resources and information Axon expects to use and will provide an initial list to Agency. Agency is responsible for and assumes the risk of any problems, delays, losses, claims, or expenses resulting from the content, accuracy, completeness, and consistency of all data, materials, and information supplied by Agency.

Axon Fleet Appendix

1 **Agency Responsibilities**. Agency must ensure its infrastructure and vehicles adhere to the minimum requirements to operate Axon Fleet 2 or Axon Fleet 3 (collectively, "Axon Fleet") as established by Axon during the qualifier call and on-site assessment at Agency and in any technical qualifying questions. If Agency's representations are inaccurate, the Quote is subject to change.

2 **Cradlepoint**. If Agency purchases Cradlepoint Enterprise Cloud Manager, Agency will comply with Cradlepoint's end user license agreement. The term of the Cradlepoint license may differ from the Axon Evidence Subscription. If Agency requires Cradlepoint support, Agency will contact Cradlepoint directly.

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

4 **Wireless Offload Server.**

4.1 **License Grant**. Axon grants Agency 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.

4.2 **Restrictions**. Agency 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.

4.3 **Updates**. If Agency 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. Agency 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.

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

5 **Axon Vehicle Software.**

5.1 **License Grant**. Axon grants Agency 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.

5.2 **Restrictions**. Agency 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.

6 **Axon Fleet Upgrade**. If Agency has no outstanding payment obligations and has purchased the "Fleet Technology Assurance Plan" (Fleet TAP), Axon will provide Agency with the same or like model of Fleet hardware ("Fleet Upgrade") as schedule on the Quote.

If Agency would like to change models for the Axon Fleet Upgrade, Agency must pay the difference between the MSRP for the offered Axon Fleet Upgrade and the MSRP for the model desired. The MSRP is the MSRP in effect at the time of the upgrade. Agency is responsible for the removal of previously installed hardware and installation of the Axon Fleet Upgrade.

Within 30 days of receiving the Axon Fleet Upgrade, Agency must return the original Axon Devices to Axon or destroy the Axon Devices and provide a certificate of destruction to Axon, including serial numbers of the destroyed Axon Devices. If Agency does not destroy or return the Axon Devices to Axon, Axon will deactivate the serial numbers for the Axon Devices received by Agency.

7 **Privacy.** Axon will not disclose Agency Content or any information about Agency except as compelled by a court or administrative body or required by any law or regulation. Axon will give notice if any disclosure request is received for Agency Content, so Agency may file an objection with the court or administrative body.

8 **Axon Fleet Termination.** Axon may terminate Agency's Fleet subscription for non-payment. Upon any termination:

8.1 Axon Fleet subscription coverage terminates, and no refunds will be given.

8.2 Axon will not and has no obligation to provide the Axon Fleet Upgrade.

8.3 Agency will be responsible for payment of any missed payments due to the termination before being allowed to purchase any future Fleet TAP.

Axon Respond Appendix

This Axon Respond Appendix applies to both Axon Respond and Axon Respond Plus.

1 **Axon Respond Subscription Term**. If Agency purchases Axon Respond as part of a bundled offering, the Axon Respond subscription begins on the later of the (1) start date of that bundled offering, or (2) date Axon provisions Axon Respond to Agency.

If Agency purchases Axon Respond as a standalone, the Axon Respond subscription begins the later of the (1) date Axon provisions Axon Respond to Agency, or (2) first day of the month following the Effective Date.

The Axon Respond subscription term will end upon the completion of the Axon Evidence Subscription associated with Axon Respond.

2 **Scope of Axon Respond**. The scope of Axon Respond is to assist Agency with real-time situational awareness during critical incidents to improve officer safety, effectiveness, and awareness. In the event Agency uses Axon Respond outside this scope, Axon may initiate good-faith discussions with Agency on upgrading Agency's Axon Respond to better meet Agency's needs.

3 **Axon Body 3 LTE Requirements**. Axon Respond is only available and usable with an LTE enabled body-worn camera. Axon is not liable if Agency utilizes the LTE device outside of the coverage area or if the LTE carrier is unavailable. LTE coverage is only available in the United States, including any U.S. territories. Axon may utilize a carrier of Axon's choice to provide LTE service. Axon may change LTE carriers during the Term without Agency's consent.

4 **Axon Fleet 3 LTE Requirements.** Axon Respond is only available and usable with a Fleet 3 system configured with LTE modem and service. Agency is responsible for providing LTE service for the modem. Coverage and availability of LTE service is subject to Agency's LTE carrier.

5 **Axon Respond Service Limitations**. Agency acknowledges that LTE service is made available only within the operating range of the networks. Service may be temporarily refused, interrupted, or limited because of: (a) facilities limitations; (b) transmission limitations caused by atmospheric, terrain, other natural or artificial conditions adversely affecting transmission, weak batteries, system overcapacity, movement outside a service area or gaps in coverage in a service area and other causes reasonably outside of the carrier's control such as intentional or negligent acts of third parties that damage or impair the network or disrupt service; or (c) equipment modifications, upgrades, relocations, repairs, and other similar activities necessary for the proper or improved operation of service.

With regard to Axon Body 3, Partner networks are made available as-is and the carrier makes no warranties or representations as to the availability or quality of roaming service provided by carrier partners, and the carrier will not be liable in any capacity for any errors, outages, or failures of carrier partner networks. Agency expressly understands and agrees that it has no contractual relationship whatsoever with the underlying wireless service provider or its affiliates or contractors and Agency is not a third-party beneficiary of any agreement between Axon and the underlying carrier.

6 **Termination**. Upon termination of this Agreement, or if Agency stops paying for Axon Respond or bundles that include Axon Respond, Axon will end Aware services, including any Axon-provided LTE service.

Add-on Services Appendix

This Appendix applies to Axon Citizen for Communities, Axon Redaction Assistant, and Axon Performance.

1 **Subscription Term**. If Agency purchases Axon Citizen for Communities, Axon Redaction Assistant, or Axon Performance as part of OSP 7, the subscription begins on the later of the (1) start date of the OSP 7 Term, or (2) date Axon provisions Axon Citizen for Communities, Axon Redaction Assistant, or Axon Performance to Agency.

If Agency purchases Axon Citizen for Communities, Axon Redaction Assistant, or Axon Performance as a standalone, the subscription begins the later of the (1) date Axon provisions Axon Citizen for Communities, Axon Redaction Assistant, or Axon Performance to Agency, or (2) first day of the month following the Effective Date.

The subscription term will end upon the completion of the Axon Evidence Subscription associated with the add-on.

2 **Axon Citizen Storage**. For Axon Citizen, Agency may store an unlimited amount of data submitted through the public portal ("**Portal Content**"), within Agency's Axon Evidence instance. The post-termination provisions outlined in the Axon Cloud Services Terms of Use Appendix also apply to Portal Content.

3 **Performance Auto-Tagging Data**. In order to provide some features of Axon Performance to Agency, Axon will need to store call for service data from Agency's CAD or RMS.

Axon Auto-Transcribe Appendix

This Appendix applies to Axon Auto-Transcribe.

1) **Subscription Term.** If Agency purchases Axon Auto-Transcribe as part of a bundle or Axon Cloud Services subscription, the subscription begins on the later of the (1) start date of the bundle or Axon Cloud Services license term, or (2) date Axon provisions Axon Auto-Transcribe to Agency. If Agency purchases Axon Auto-Transcribe minutes as a standalone, the subscription begins on the date Axon provisions Axon Auto-Transcribe to Agency.

   Axon Auto-Transcribe minutes expire one year after being provisioned to Agency by Axon.

   If Agency cancels Auto-Transcribe services, any amounts owed by the Parties will be based on the amount of time passed under the annual subscription, rather than on the number of minutes used, regardless of usage.

2) **Auto-Transcribe A-La-Carte Minutes.** Upon Axon granting Agency a set number of minutes, Agency may utilize Axon Auto-Transcribe, subject to the number of minutes allowed on the Quote. Agency will not have the ability to roll over unused minutes to future Auto-Transcribe terms. Axon may charge Agency additional fees for exceeding the number of purchased minutes.

3) **Axon Auto-Transcribe On-Demand.** Upon Axon granting Agency an On-Demand subscription to Axon Auto-Transcribe, Agency may utilize Axon Auto-Transcribe with no limit on the number of minutes. The scope of Axon Auto-Transcribe On-Demand is to assist Agency with reviewing and transcribing individual evidence items. In the event Agency uses Axon Auto-Transcribe On-Demand outside this scope, Axon may initiate good-faith discussions with Agency on upgrading Agency's Axon Auto-Transcribe On-Demand to better meet Agency's needs.

4) **Warranty.** Axon does not warrant the accuracy of Axon Auto-Transcribe.

Axon Virtual Reality Content Terms of Use Appendix

1 **Term**. The Quote will detail the duration of the Virtual Reality Content license.

2 **Headsets**. Agency may purchase additional virtual reality headsets from Axon. In the event Agency decides to purchase additional virtual reality headsets for use with Axon's Virtual Reality Content, Agency must purchase those headsets from Axon.

3 **License Restrictions**. All licenses will immediately terminate if Agency does not comply with any term of this Agreement. If Agency utilizes more users than stated in this Agreement, Agency must purchase additional Virtual Reality Content licenses from Axon. Agency may not use Virtual Reality Content for any purpose other than as expressly permitted by this Agreement. Agency may not:

- **3.1** modify, tamper with, repair, or otherwise create derivative works of Virtual Reality Content;
- **3.2** reverse engineer, disassemble, or decompile Virtual Reality Content or apply any process to derive the source code of Virtual Reality Content, or allow others to do the same;
- **3.3** copy Virtual Reality Content in whole or part, except as expressly permitted in this Agreement;
- **3.4** use trade secret information contained in Virtual Reality Content;
- **3.5** resell, rent, loan or sublicense Virtual Reality Content;
- **3.6** access Virtual Reality Content to build a competitive device or service or copy any features, functions, or graphics of Virtual Reality Content; or
- **3.7** remove, alter, or obscure any confidentiality or proprietary rights notices (including copyright and trademark notices) of Axon or Axon's licensors on or within Virtual Reality Content or any copies of Virtual Reality Content.

4 **Termination**. Axon may terminate Agency's license immediately for Agency's failure to comply with any of the terms in this Agreement.

Skydio Terms of Use Appendix

1 **Definitions**.

"**Advanced Software**" means optional capabilities, functions or other features of the Onboard Software that may be specified and identified as such in the Quote. Skydio's characterization of capabilities, functions or other features as Advanced Software shall be dispositive. Notwithstanding any other provision herein, a software feature that is locked or otherwise disabled unless or until an Advanced Software Package is purchased for such software feature shall be deemed an Advanced Software. Advanced Software does not include Mobile Apps.

"**Advanced Software Package**" means an optional, additional-charge license right, specified in the Quote, pursuant to which Skydio shall unlock Advanced Software to permit Customer to use Advanced Software (and in some cases the Skydio Hardware that it controls).

"**Authorized Devices**" are (a) mobile devices that Customer owns or is authorized to use, and (b) controllers purchased by Customer hereunder, which in each case (a) and (b) are used by Customer to operate the Skydio Hardware purchased by Customer hereunder.

"**Base Software**" means capabilities, functions or other features of the Onboard Software that are both: (a) standard capabilities, functions or other features available and activated on Skydio's base consumer version of Skydio Hardware, and (b) available for use without purchase of Advanced Software Package. Base Software may be specified and identified as standard features in the Quote. Any capability, function, or feature that is not a Base Software shall be deemed an Advanced Software.

"**Customer**" means the customer procuring Skydio Products or services.

"**Error**" means a critical error in the Advanced Software that causes the Advanced Software to be inoperable.

"**Skydio License Term**" means with respect to an Advanced Software Package, the term of that Advanced Software Package, including (if applicable) the initial specified term and any renewal terms.

"**Mobile Apps**" means software applications (in executable form only), as may be specified on the Quote, that are specifically intended for use on a mobile device (and any Updates thereto).

"**Onboard Software**" means software, in executable format only, embedded into or otherwise pre-installed on Skydio Hardware as supplied by Skydio, and any Updates thereto, whether or not embedded on read only memory. Onboard Software includes Base Software and Advanced Software.

"**Skydio Privacy Policy**" means Skydio's privacy policy located at https://www.skydio.com/privacy-policy and as it may be amended from time to time by Skydio in its sole discretion.

"**Product**" means Skydio Hardware and Software, as provided by Skydio pursuant to this Agreement and any applicable Quote.

"**Skydio Hardware**" means drones and other unmanned aircraft, controllers, docks, accessories and related hardware that Customer purchases from Skydio or its distributors or resellers.

"**Skydio Software**" means Onboard Software and Mobile Apps.

"**Support Term**" means, for Base Software, the support term specified in the Quote, and, for each Advanced Software Package, the applicable Skydio License Term for such Advanced Software

Package purchased hereunder.

"**Updates**" means any upgrades, updates, maintenance releases, bug fixes or modified versions of Skydio Software that Skydio may release from time to time.

2 **License**. Subject to and in accordance with the terms and conditions of this Agreement and further conditioned upon Customer's payment of all Fees, Skydio grants to Customer:

2.1 a limited, perpetual, non-exclusive, non-transferable (except as provided in Section 5 below titled "Transferability") right and license to use the Base Software solely on Skydio Hardware;

2.2 a limited, perpetual, non-exclusive, non-transferable right and license to download, install, execute and use Mobile Apps on Authorized Devices solely to operate Skydio Hardware in accordance with this Agreement;

2.3 if Customer purchases an Advanced Software Package for the use of an Advanced Software, as specified in the Quote, a limited, non-exclusive, non-transferable right and license, during the Skydio License Term of the Advanced Software Package, to use the Advanced Software on Skydio Hardware that Customer purchases from Skydio solely to operate the Skydio Hardware in accordance with this Agreement ("**Advanced Software License"**); and

2.4 a limited, non-exclusive, non-transferable right and license to install solely on Skydio Hardware any Updates to the Onboard Software, if and when provided by Skydio.

3 **Additional License Terms**. Additional License Terms. The license rights of Section 2 are limited to the United States, Canada and Japan.

3.1 Unless otherwise specified in the applicable Quote, the Advanced Software License is granted on a per-unit basis and it may only be exercised with respect to the specific units of Skydio Hardware identified on the applicable Quote or, if the Quote does not specify such units, then with respect to no more than the total number of Skydio Hardware units authorized on the Quote, or if such total number of units is not specified on the Quote, then only with respect to one (1) single Skydio Hardware unit ("**Authorized Units**").

3.2 Rights under the Advanced Software License are not transferable between Authorized Units. When an Advanced Software License is exercised on a specific Authorized Unit (by unlocking, activating, accessing or using the Advanced Software on that Authorized Unit), such Advanced Software License, or any rights thereof, cannot be transferred to a different unit of Skydio Hardware, except: (i) if Skydio replaces an Authorized Unit pursuant to a warranty claim, Skydio shall transfer to the replacement Authorized Unit, the Advanced Software License of the inoperable unit that is being replaced, and (ii) if a particular Authorized Unit is rendered permanently inoperable, Skydio shall, upon Customer's request, transfer the Advanced Software License rights to a replacement Authorized Unit, provided, however, that Skydio may condition such transfer on Customer returning to Skydio the remnants of the inoperable unit or other evidence of its inoperability.

4 **Limitations and Restrictions**. Except as otherwise expressly provided in this Agreement, the foregoing license grant excludes any right to, and Customer shall not (and shall not permit others to) do any of the following with respect to the Skydio Software: (i) license, sublicense, sell, resell, rent, lease, transfer, distribute, time share, operate as a service bureau, or otherwise make any of it available for access by third parties; (ii) disassemble, reverse engineer or decompile it; (iii) copy, create derivative works based on or otherwise modify it; (iv) remove or modify a copyright, trademark, logo or other proprietary rights notice or brand labeling in it; (v) use it to reproduce, distribute, display, transmit, or use material protected by copyright or other intellectual property right (including the rights of publicity or privacy) without first obtaining the permission of the owner; (vi) use it to create, use, send, store or run viruses or other harmful computer code, files, scripts, agents or other programs or otherwise engage, in a malicious act or disrupt its security, integrity or operation; (vii) install, execute or otherwise reproduce Onboard Software on any device other than the Skydio Hardware on which Skydio originally installed the Onboard Software; (viii) install any

Skydio Software on any type of device not approved by Skydio; (ix) disable or otherwise circumvent any technological measures in Skydio Software to limit its installation, use or access; (x) unlock, activate, access or use an Advanced Software on any device other than as permitted under an Advanced Software Package purchased by Customer; and (xi) publish or release any benchmarking or performance data applicable to the Skydio Software.

5 **Transferability**. Subject to the terms and conditions of this Agreement, Customer may transfer the Base Software, including any relevant Base Software license rights, only on a permanent basis and as part of the sale or transfer of the Skydio Hardware on which the Base Software is loaded, provided that Customer retains no copies of any version of the Skydio Software. With the exception of the Base Software, Customer may not transfer any other Skydio Software or other Skydio Software license rights granted herein to another person or entity without the express written permission of Skydio, unless allowed by applicable law stating that transfer may not be restricted.

6 **Evaluation License**. Skydio may make certain Skydio Software available in object code form to end users only for evaluation, training or other limited non-commercial purposes without charging a Fee ("**Evaluation License**"). Where Skydio has provided an Evaluation License, all of the terms of this Agreement shall apply except that (i) Customer's license rights shall be limited to the evaluation of that Skydio Software, (ii) Customer shall not be required to pay a Fee for the evaluation of that Skydio Software and (iii) Skydio shall have the right to revoke the license to the Skydio Software at any time and for any reason.

7 **Updates**. The terms and conditions of this Agreement shall apply to all Updates or additional copies of the Skydio Software. Subject to the terms and conditions of this Agreement, including Customer's timely payment of all Fees due and owed to Skydio, Skydio will provide or make available to Customer, during the Support Term, Updates for Base Software, Mobile Apps and any Advanced Software that was enabled under the purchased Advanced Software Package on the Authorized Units. Notwithstanding any other provision of this Agreement, Customer has no license or right to use any Updates to the Advanced Software unless Customer holds a valid license to the Advanced Software and has paid any required Fees for such Advanced Software. Updates are solely provided on a "when-and-if-available" basis and as made generally available by Skydio to its customers. Customer shall promptly install any Updates that Skydio designates as required for the continued safe operation of Skydio Hardware or operation of any Advanced Software.

8 **Proprietary Notices**. Customer agrees to maintain and reproduce all copyright and other proprietary notices on all copies, in any form, of the Skydio Software in the same form and manner that such copyright and other proprietary notices are included on the Skydio Software.

9 **Intellectual Property**. Customer agrees that all worldwide patent, copyright and other intellectual property rights in the Product, and all copies of the Software however made (including copies pre-installed on the Skydio Hardware purchased by Customer) are the exclusive property of Skydio and its suppliers. All Skydio Software is licensed to Customer, not sold. All rights not expressly granted to Customer in this Agreement are reserved by Skydio and its suppliers. There are no implied licenses under this Agreement.

10 **Fees**. Skydio reserves the right to suspend and/or terminate access to the Skydio Software if any undisputed fees for Skydio Hardware or Software are past due. Such suspension or termination shall not relieve Customer from its obligation to pay all undisputed amounts.

11 **Third Party Software and Open Source Software**. The Skydio Software may include third party software, and open source software ("**OSS**"), and such software is provided under separate license terms.

11.1 To the extent the licenses for any OSS requires Skydio to make available to Customer the corresponding source code included in the Skydio Software, Customer may obtain a copy of the applicable OSS source code by sending a written request to legal@skydio.com. The

OSS license terms shall take precedence over this Agreement to the extent that this Agreement imposes greater restrictions on Customer than the applicable OSS license terms. Customer acknowledges receipt of notices for the Open Source Components for the initial delivery of the Skydio Software.

11.2 The use of third party software or applications, or the integration of such software or applications with the Skydio Software, (collectively, "**Third Party Applications**"), may result in Customer data or information being transferred to a third party. Skydio is not responsible for, and Customer agrees to hold Skydio harmless, for any data or information transferred to third parties in connection with your use of Third Party Applications.

12 **Commercial Item.** The Skydio Software and associated documentation are "commercial items" as defined at FAR 2.101 and according to DFAR section 252.2277014(a)(1) and (5) are deemed to be "commercial computer software" and "commercial computer software documentation." Consistent with DFAR section 227.7202 and FAR section 12.212, any use, modification, reproduction, release, performance, display, or disclosure of such commercial software or commercial software documentation by the U.S. Government will be governed solely by the terms of this Agreement and will be prohibited except to the extent expressly permitted by the terms of this Agreement.

13 **Term and Termination.** This Agreement is effective upon Skydio Software purchase, activation or download, as applicable, and shall continue until terminated.

13.1 **Paid License Term**. Each Advanced Software Package purchased hereunder shall have its own Skydio License Term. Each Skydio License Term shall have an initial term for the time period set forth on the Quote and that the Skydio License Term shall automatically extend for successive additional one (1) year renewal terms thereafter if any (subject to payment of the then-current applicable license fees for each such renewal term) unless either party give notice to the other of its intention not to renew the Skydio License Term at least thirty (30) days before expiration of the then-current initial or renewal term, as the case may be ("**Renewal Terms**"). If a Skydio License Term is not set forth in the Quote, each Skydio License Term shall have an initial term that commences upon the date of provisioning of the Skydio Software and expires one (1) year later; provided, however, that the Skydio License Term shall automatically extend per the Renewal Terms. Unless Skydio terminates this Agreement for breach by Customer, the perpetual licenses to use Base Software shall survive.

13.2 **Free or Trial License Term**. If you have obtained a license to a free version of the Skydio Software, then your license will continue until terminated in accordance with this Agreement. If you have obtained a trial license to the Skydio Software, then your license will continue for such time period as may be specified by Skydio with respect to such trial (and if no period is specified, for 30 days). Skydio may terminate a trial license at any time in its sole discretion.

13.3 **Termination**. Skydio may terminate Customer's license rights under this Agreement immediately without notice if Customer fails to comply with any terms of this Agreement or Customer fails to make any payment as required hereunder. In no event will termination relieve Customer of its obligation to pay any fees payable for Skydio Hardware or Software. Upon termination or expiration of this Agreement for any reason, Customer shall immediately cease using any Skydio Software and must destroy or return to Skydio all copies of the Skydio Software and associated documentation in its possession or control. The following sections shall survive the termination or expiration of this Agreement: Sections 1, 2(a), 2(b), 2(d), 4, 5 and 7-26.

14 **End of Life**. Skydio may discontinue the provision of any Skydio Software, support or Updates in its sole discretion in accordance with, and any licenses granted herein are subject to, Skydio

Product End of Life Policy, which is available at https://support.skydio.com/hc/en-us/articles/360057153714, and is hereby incorporated by reference herein.

15 **Limited Warranty.** The only warranty that Skydio provides with respect to any Skydio products or services is the written limited warranty statement provided with the products or services or as otherwise set forth at https://skydio.com/warranty-terms ("**Limited Warranty**").

16 **Limitations.** Any use of the Skydio Hardware and Software, including any reliance upon or use of any of the information generated thereby, shall be at Customer's and its authorized users' sole risk. Except as expressly set forth in the Limited Warranty and to the extent permitted by law, the Products are provided "as is" and "as available" without warranty of any kind (all of which are hereby disclaimed), whether express, implied or statutory, including the implied warranties of merchantability, fitness for a particular purpose, or non-infringement. If statutory or implied warranties cannot be lawfully disclaimed, then such warranties are limited to the duration of the warranty set forth in the Limited Warranty and by the provisions in this Agreement. Skydio's cumulative liability to any Party for any loss or damage resulting from any claim, demand, or action arising out of or relating to any Skydio Products or any service will not exceed the amounts paid by Customer in the 12 months prior to the action giving rise to the liability. Neither Party will be liable for direct, special, indirect, incidental, punitive or consequential damages, however caused, whether for breach of warranty or contract, negligence, strict liability, tort or any other legal theory.

17 **Safety and Compliance**. Any use of the Skydio Hardware shall comply with all laws. Any use of the Skydio Hardware by Customer and its authorized users shall be in accordance with the information and warnings set forth at https://www.skydio.com/safety (the "**Safety and Operating Guide**"). Customer acknowledges that improper operation of the unmanned aircraft systems may cause injury to persons or property. Customer shall at all times comply with all applicable local, state, national, and international laws and regulations related to the operation of unmanned aircraft systems in any territory of operation, including any applicable laws and orders with regard to privacy, pilot licensure, operating within visual line of sight (unless the Customer has received proper approval from a civil aviation authority waiving such limitation), detecting and avoiding other aircraft, and airspace restrictions (such as temporary flight restrictions issued by Federal Aviation Administration or other appropriate government agencies). Customer shall obtain and maintain all necessary licenses, consent, and authorizations of any kind necessary to operate unmanned aircraft systems.

18 **Feedback**. If Customer or Customer's authorized users send Skydio comments, suggestions, ideas, materials, notes, drawings, concepts or other information (collectively, "**Submissions**"), Customer and Customer's authorized users (as applicable) grant to Skydio a worldwide, non-exclusive, perpetual, irrevocable, transferable, sub-licensable, royalty-free license to use, copy, modify, publicly display, publicly perform, distribute and otherwise exploit the Submissions. None of the Submissions shall be subject to any obligation of confidentiality on Skydio's part, and Skydio shall not be liable for any use or disclosure of any Submissions.

19 **Privacy**. Skydio shall, in providing the Products, comply with Skydio Privacy Policy to the extent that Customer provides Skydio with personally identifiable information.

20 **Mapbox Terms.** The Mobile App uses features and content provided by Mapbox, such as maps and locations on a map. Use of any such Mapbox features and content is subject to the then-current version of Mapbox's terms and privacy policy, which can be found at https://www.mapbox.com/legal/tos/ , including the Mapbox Government Terms of Service, which can be found at https://www.mapbox.com/legal/usg-tos, and you hereby agree to comply with such terms. You can opt out of location telemetry reporting pursuant to such terms.

21 **Services.** In accordance with this Agreement, so long as Customer timely pays all amounts owed hereunder, Skydio shall render to Customer, during the applicable Skydio License Term of each

Advanced Software Package purchased herunder, the support services consisting of: (a) providing Customer's named Administrators (defined below) with consultation in English, via telephone and email, during Skydio's normal business hours (9AM to 5PM PST) to assist in using the Advanced Software licensed under the Advanced Software Package; and (b) making reasonable efforts to correct any critical error in the Advanced Software that causes the Advanced Software to be inoperable ("**Error**"), all in accordance with Skydio's support policies published on its Website, as updated from time to time. Errors do not include, and Skydio has no obligation to correct, malfunctions caused in whole or in part by modification of Software, the operation of third-party products or the integration of Software with or into third-party products, improper installation of the Advanced Software or other Software, or the use of Software other than in accordance with the applicable specifications provided by Skydio. Support is only available for the current and single prior major release of Advanced Software. No other services are included under this Agreement.

22 **Administrators.** Customer shall designate up to three (3) of its employees to administer the Services on its behalf and serve as points of contact in communicating with us, as set forth in the applicable Confirmation or as otherwise agreed by the parties in writing ("**Administrators**"). If a person named as an Administrator leaves Customer's employ, Customer may designate another one of its employees to serve as Administrator to replace the departing employee.

23 **Indemnification.** Skydio will indemnify Customer's officers, directors, and employees ("**Customer Indemnitees**") against all claims, demands, losses, and reasonable expenses arising out of a third-party claim against an Customer Indemnitee resulting from any negligent act, error or omission, or willful misconduct by Skydio under this Agreement, except to the extent of Customer's negligence or willful misconduct, or claims under workers compensation.

24 **IP Indemnification.** Skydio will indemnify Customer Indemnitees against all claims, losses, and reasonable expenses from any third-party claim alleging that the use of Skydio Products or services infringes or misappropriates the third-party's intellectual property rights. Customer must promptly provide Skydio with written notice of such claim, tender to Skydio the defense or settlement of such claim at Skydio's expense and cooperate fully with Skydio in the defense or settlement of such claim. Skydio's IP indemnification obligations do not apply to claims based on (a) modification of Skydio Products or services by Customer or a third-party not approved by Skydio; (b) use of Skydio Products and services in combination with hardware or services not approved by Skydio; (c) use of Skydio Products and services other than as permitted in this Agreement; or (d) use of Skydio Software that is not the most current release provided by Skydio.

25 **Customer Responsibilities.** Customer is responsible for (a) Customer's use of Skydio Products; (b) breach of this Agreement or violation of applicable law by Customer or a Customer's authorized end user; and (c) a dispute between Customer and a third-party over Customer's use of Skydio Products.

26 **Export Sales and Export Controls.** Customer acknowledges that the Skydio Products, services and technology are subject to export controls under the laws and regulations of the United States (U.S.). Customer shall comply with such laws and regulations governing use, export, re-export, and transfer of Skydio Products, services and technology and shall obtain all required U.S. and local authorizations, permits, or licenses. Skydio and Customer each agree to provide the other such information and assistance as may reasonably be required by the other in connection with securing such authorizations and licenses, and to take timely action to obtain all required supporting documentation.

* * * *

Skydio, Inc.
114 Hazel Ave.,
Redwood City, CA 94061
legal@skydio.com

Axon Commander™ Software Appendix

5 **License**. Axon owns all executable instructions, images, icons, sound, and text in Commander. All rights are reserved to Axon. Axon grants a non-exclusive, royalty-free, worldwide right and license to use Commander. "Use" means storing, loading, installing, or executing Commander exclusively for data communication with an Axon Device. Agency may use Commander in a networked environment on computers other than the computer it installs Commander on, so long as each execution of Commander is for data communication with an Axon Device. Agency may make copies of Commander for archival purposes only. Agency shall retain all copyright, trademark, and proprietary notices in Commander on all copies or adaptations.

6 **Term**. The Quote will detail the duration of the Commander license, as well as any maintenance. The term will begin upon installation of Commander by Axon.

7 **License Restrictions**. All licenses will immediately terminate if Agency does not comply with any term of this Agreement. Agency may not use Commander for any purpose other than as expressly permitted by this Agreement. Agency may not:

7.1 modify, tamper with, repair, or otherwise create derivative works of Commander;
7.2 reverse engineer, disassemble, or decompile Commander or apply any process to derive the source code of Commander, or allow others to do the same;
7.3 access or use Commander to avoid incurring fees or exceeding usage limits or quotas;
7.4 copy Commander in whole or part, except as expressly permitted in this Agreement;
7.5 use trade secret information contained in Commander;
7.6 resell, rent, loan or sublicense Commander;
7.7 access Commander to build a competitive device or service or copy any features, functions, or graphics of Commander; or
7.8 remove, alter, or obscure any confidentiality or proprietary rights notices (including copyright and trademark notices) of Axon or Axon's licensors on or within Commander or any copies of Commander.

8 **Support**. Axon may make available updates and error corrections ("**Updates**") to Commander. Axon will provide Updates electronically via the Internet or media as determined by Axon. Agency is responsible for establishing and maintaining adequate access to the Internet to receive Updates. Agency is responsible for maintaining the computer equipment necessary to use Commander. Axon may provide technical support of a prior release/version of Commander for 6 months from when Axon made the subsequent release/version available.

9 **Termination**. Axon may terminate Agency's license immediately for Agency's failure to comply with any of the terms in this Agreement. Upon termination, Axon may disable Agency's right to login to Axon Commander.

Axon Application Programming Interface Appendix

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

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

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

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

2 **Purpose and License**.
2.1 Agency may use API Service and data made available through API Service, in connection with an API Client developed by Agency. Axon may monitor Agency's use of API Service to ensure quality, improve Axon devices and services, and verify compliance with this Agreement. Agency agrees to not interfere with such monitoring or obscure from Axon Agency's use of API Service. Agency will not use API Service for commercial use.
2.2 Axon grants Agency a non-exclusive, non-transferable, non-sublicensable, worldwide, revocable right and license during the Term to use API Service, solely for Agency's Use in connection with Agency's API Client.
2.3 Axon reserves the right to set limitations on Agency'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**. Agency will work independently to configure Agency's API Client with API Service for Agency's applicable Use. Agency 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. Agency will inform Axon promptly of any updates. Upon Agency's registration, Axon will provide documentation outlining API Service information.

4 **Agency Responsibilities**. When using API Service, Agency and its end users may 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 viruses, worms, defect, Trojan horses, malware, or any items 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 disclose Axon's API manual.

5 **API Content**. All content related to API Service, other than Agency Content or Agency'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 Agency takes actions on, such as evidence, cases, users, or reports; and
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 Agency 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**"). Agency is required to implement and use the most current version of API Service and to make any applicable changes to Agency's API Client required as a result of such API Update. API Updates may adversely affect how Agency's API Client access or communicate with API Service or the API Interface. Each API Client must contain means for Agency to update API Client to the most current version of API Service. Axon will provide support for 1 year following the release of an API Update for all depreciated API Service versions.

Advanced User Management Appendix

1 **Scope**. Advanced User Management allows Agency to (a) utilize bulk user creation and management, (b) automate user creation and management through System for Cross-domain Identity Management ("**SCIM**"), and (c) automate group creation and management through SCIM.

2 **Advanced User Management Configuration**. Agency will work independently to configure Agency's Advanced User Management for Agency's applicable Use. Upon request, Axon will provide general guidance to Agency, including documentation that details the setup and configuration process.

Axon Channel Services Appendix

1 **Definitions**.
"**Axon Digital Evidence Management System**" means Axon Evidence or Axon Commander, as specified in the attached Channel Services Statement of Work.

"**Active Channel**" means a third-party system that is continuously communicating with an Axon Digital Evidence Management System.

"**Inactive Channel**" means a third-party system that will have a one-time communication to an Axon Digital Evidence Management System.

2 **Scope**. Agency currently has a third-party system or data repository from which Agency desires to share data with Axon Digital Evidence Management. Axon will facilitate the transfer of Agency's third-party data into an Axon Digital Evidence Management System or the transfer of Agency data out of an Axon Digital Evidence Management System as defined in the Channel Services Statement of Work ("**Channel Services SOW**"). Channel Services will not delete any Agency Content. Agency is responsible for verifying all necessary data is migrated correctly and retained per Agency policy.

3 **Purpose and Use**. Agency is responsible for verifying Agency has the right to share data from and provide access to third-party system as it relates to the Services described in this Appendix and the Channel Services SOW. For Active Channels, Agency is responsible for any changes to a third-party system that may affect the functionality of the channel service. Any additional work required for the continuation of the Service may require additional fees. An Axon Field Engineer may require access to Agency's network and systems to perform the Services described in the Channel Services SOW. Agency is responsible for facilitating this access per all laws and policies applicable to Agency.

4 **Project Management**. Axon will assign a Project Manager to work closely with Agency's project manager and project team members and will be responsible for completing the tasks required to meet all contract deliverables on time and budget.

5 **Warranty.** Axon warrants that it will perform the Channel Services in a good and workmanlike manner.

6 **Monitoring**. Axon may monitor Agency's use of Channel Services to ensure quality, improve Axon devices and services, prepare invoices based on the total amount of data migrated, and verify compliance with this Agreement. Agency agrees not to interfere with such monitoring or obscure from Axon Agency's use of channel services.

7 **Agency's Responsibilities.** Axon's successful performance of the Channel Services requires Agency:

7.1 Make available its relevant systems for assessment by Axon (including making these systems available to Axon via remote access);

7.2 Provide access to the building facilities and where Axon is to perform the Channel Services, subject to safety and security restrictions imposed by the Agency (including providing security passes or other necessary documentation to Axon representatives performing the Channel Services permitting them to enter and exit Agency premises with laptop personal computers and any other materials needed to perform the Channel Services);

7.3 Provide all necessary infrastructure and software information (TCP/IP addresses, node names, and network configuration) for Axon to provide the Channel Services;

7.4 Ensure all appropriate data backups are performed;

7.5 Provide Axon with remote access to the Agency's network and third-party systems when required for Axon to perform the Channel Services;

7.6 Notify Axon of any network or machine maintenance that may impact the performance of

the Channel Services; and

7.7 Ensure the reasonable availability by phone or email of knowledgeable staff, personnel, system administrators, and operators to provide timely, accurate, complete, and up-to-date documentation and information to Axon (these contacts are to provide background information and clarification of information required to perform the Channel Services).

VIEVU Data Migration Appendix

1 **Scope**. Agency currently has legacy data in the VIEVU Solution from which Agency desires to move to Axon Evidence. Axon will work with Agency to copy legacy data from the VIEVU solution into Axon Evidence ("**Migration**"). Before Migration, Agency and Axon will work together to develop a Statement of Work ("**Migration SOW**") to detail all deliverables and responsibilities. The Migration will require the availability of Agency resources. Such resources will be identified in the SOW. On-site support during Migration is not required. Upon Agency's request, Axon will provide on-site support for an additional fee. Any request for on-site support will need to be pre-scheduled and is subject to Axon's resource availability.

A small amount of unexposed data related to system information will not be migrated from the VIEVU solution to Axon Evidence. Upon request, some of this data can be manually exported before Migration and provided to Agency. The Migration SOW will provide further detail.

2 **Changes**. Axon is only responsible to perform the Services described in this Appendix and Migration SOW. Any additional services are out of scope. The Parties must document scope changes in a written and signed change order. Changes may require an equitable adjustment in the charges or schedule.

3 **Project Management**. Axon will assign a Project Manager to work closely with Agency's project manager and project team members and will be responsible for completing the tasks required to meet all contract deliverables on time and budget.

4 **Downtime**. There may be downtime during the Migration. The duration of the downtime will depend on the amount of data that Agency is migrating. Axon will work with Agency to minimize any downtime. Any VIEVU mobile application will need to be disabled upon Migration.

5 **Functionality Changes**. Due to device differences between the VIEVU solution and the Axon's Axon Evidence solution, there may be functionality gaps that will not allow for all migrated data to be displayed the same way in the user interface after Migration

6 **Acceptance**. Once the Migration is complete, Axon will notify Agency and an acceptance form. Agency is responsible for verifying that the scope of the project has been completed and all necessary data is migrated correctly and retained per Agency policy. Agency will have 90 days to provide Axon acceptance that the Migration was successful, or Axon will deem the Migration accepted.

In the event Agency does not accept the Migration, Agency agrees to notify the Axon within a reasonable time. Agency also agrees to allow Axon a reasonable time to resolve any issue. In the event Agency does not provide the Axon written rejection of the Migration during these 90 days, Agency may be charged for additional monthly storage costs. After Agency provides acceptance of the Migration, the Axon will delete all data from the VIEVU solution 90 days after the Migration.

7 **Post-Migration**. After Migration, the VIEVU solution may not be supported and updates may not be provided. Axon may end of life the VIEVU solution in the future. If Agency elects to maintain data within the VIEVU solution, Axon will provide Agency 90 days' notice before ending support for the VIEVU solution.

8 **Warranty.** Axon warrants that it will perform the Migration in a good and workmanlike manner.

9 **Monitoring**. Axon may monitor Agency's use of Migration to ensure quality, improve Axon devices and services, prepare invoices based on the total amount of data migrated, and verify compliance with this Agreement. Agency agrees not to interfere with such monitoring or obscure from Axon Agency's use of Migration.

Axon Support Engineer Appendix

1 **Axon Support Engineer Payment.** Axon will invoice for Axon Support Engineer ("**ASE**") services, as outlined in the Quote, when the Axon Support Engineer commences work on-site at Agency.

2 **Full-Time ASE Scope of Services.**

2.1 A Full-Time ASE will work on-site four (4) days per week.

2.2 Agency's Axon sales representative and Axon's Agency Success team will work with Agency to define its support needs and ensure the Full-Time ASE has skills to align with those needs. There may be up to a 6-month waiting period before the Full-Time ASE can work on-site, depending upon Agency's needs and availability of a Full-Time ASE.

2.3 The purchase of Full-Time ASE Services includes 2 complimentary Axon Accelerate tickets per year of the Agreement, so long as the ASE has started work at Agency, and Agency is current on all payments for the Full-Time ASE Service.

The Full-Time ASE Service options are listed below:

Ongoing System Set-up and Configuration • Assisting with assigning cameras and registering docks • Maintaining Agency's Axon Evidence account • Connecting Agency to "Early Access" programs for new devices
Account Maintenance • Conducting on-site training on new features and devices for Agency leadership team(s) • Thoroughly documenting issues and workflows and suggesting new workflows to improve the effectiveness of the Axon program • Conducting weekly meetings to cover current issues and program status
Data Analysis • Providing on-demand Axon usage data to identify trends and insights for improving daily workflows • Comparing Agency's Axon usage and trends to peers to establish best practices • Proactively monitoring the health of Axon equipment and coordinating returns when needed
Direct Support • Providing on-site, tier 1 and tier 2 technical support for Axon devices • Proactively monitoring the health of Axon equipment • Creating and monitoring RMAs on-site • Providing Axon app support • Monitoring and testing new firmware and workflows before they are released to Agency's production environment
Agency Advocacy • Coordinating bi-annual voice of customer meetings with Axon's Device Management team • Recording and tracking Agency feature requests and major bugs

3 **Regional ASE Scope of Services**

3.1 A Regional ASE will work on-site for 3 consecutive days per quarter. Agency must schedule the on-site days at least 2 weeks in advance. The Regional ASE will also be available by phone and email during regular business hours up to 8 hours per week.

3.2 There may be up to a 6-month waiting period before Axon assigns a Regional ASE to Agency, depending upon the availability of a Regional ASE.

3.3 The purchase of Regional ASE Services includes 2 complimentary Axon Accelerate tickets per year of the Agreement, so long as the ASE has started work at Agency and Agency is current on all payments for the Regional ASE Service.

The Regional ASE service options are listed below:

Account Maintenance • Conducting remote training on new features and devices for Agency's leadership • Thoroughly documenting issues and workflows and suggesting new workflows to improve the effectiveness of the Axon program • Conducting weekly conference calls to cover current issues and program status • Visiting Agency quarterly (up to 3 consecutive days) to perform a quarterly business review, discuss Agency's goals for your Axon program, and continue to ensure a successful deployment of Axon devices
Direct Support • Providing remote, tier 1 and tier 2 technical support for Axon devices • Creating and monitoring RMAs remotely
Data Analysis • Providing quarterly Axon usage data to identify trends and program efficiency opportunities • Comparing an Agency's Axon usage and trends to peers to establish best practices • Proactively monitoring the health of Axon equipment and coordinating returns when needed
Agency Advocacy • Coordinating bi-yearly Voice of Agency meetings with Device Management team • Recording and tracking Agency feature requests and major bugs

4 **Out of Scope Services.** The ASE is responsible to perform only the Services described in this Appendix. Any additional Services discussed or implied that are not defined explicitly in this Appendix will be considered out of the scope.

5 **ASE Leave Time**. The ASE will be allowed up 7 days of sick leave and up to 15 days of vacation time per each calendar year. The ASE will work with Agency to coordinate any time off and will provide Agency with at least 2 weeks' notice before utilizing any vacation days.

AXON CLOUD SERVICES PRIVACY POLICY

Last Updated: August 9th, 2021

*This Axon Cloud Services Privacy Policy ("**Policy**") applies only to the information that Axon Enterprise, Inc. ("**Axon**") collects and you or your employer (collectively, "**Customer**") 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 Privacy Policy. Usage of Axon Citizen is governed by the Axon Citizen Privacy Policy.*

Unless otherwise provided in this Policy, this Policy is subject to the terms of the Master Services Purchasing Agreement, or other similar agreement, if any, between Axon and Customer ("**Agreement**"). To the extent this Policy contains terms and conditions that differ from those contained in the Agreement, the Agreement shall control. A concept or principle covered in this Policy 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 and defined terms referenced, but not defined, in this Policy shall have the meanings assigned to them in the Agreement.

Axon complies with the EU-U.S. Privacy Shield Framework and the Swiss-U.S. Privacy Shield Framework ("Privacy Shield") as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal information transferred from the European Union, the United Kingdom, and Switzerland to the United States in reliance on Privacy Shield. Axon has certified to the U.S. Department of Commerce that it adheres to the Privacy Shield Principles with respect to such information. If any conflict exists between the terms of this Policy and the Privacy Shield Principles, the Privacy Shield Principles shall govern. To learn more about the Privacy Shield program, and to view our certification, please visit https://www.privacyshield.gov/.

By using Axon Cloud Services, Customer acknowledges that Customer has read and understand this Policy and Customer agrees to be bound by its terms and conditions. Axon may occasionally update this Policy. 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 agreement and acceptance to any such changes.

Definitions

- "**Axon Cloud Services**" means Axon's web services hosted on evidence.com including **Axon Evidence**, **Axon Records,** and **Axon Dispatch**, 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 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 and users;
(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.

For purposes of clarity, Customer Content does not include Non-Content Data, and Non-Content Data does not include Customer Content.

- **“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.
- **“Data Exporter”** means the Data Controller who transfers the Personal Data.
- **“Data Importer”** means the Data Processor who agrees to receive from the Data Exporter Personal Data intended for processing on Data Exporter's behalf after the transfer in accordance with the Agreement and who is not subject to a third country’s system ensuring adequate protection with in the meaning of the General Data Protection Regulation (EU) 2016/679 of the European Parliament (“**GDPR**”)
- **“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.
- “**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 processor engaged by the Data Importer or by any other sub-processor of the Data Importer who agrees to receive from the Data Importer or from any other sub-processor of the Data Importer Personal Data exclusively intended for processing activities to be carried out on behalf of the Data Exporter after the transfer in accordance with its instructions, the terms of the Clauses and the terms of the written subcontract.

Axon's Role

Axon is a Data Processor of Customer Content. Customer controls and owns all right, title, and interest in and to Customer Content and Axon obtains no rights to the Customer Content. Customer is solely responsible for the uploading, sharing, withdrawal, management and deletion of Customer Content. Customer grants Axon limited access to Customer Content solely to provide and support Axon Cloud Services to and for Customer and Customer's end-users. Customer represents and warrants to Axon that: (1) Customer owns Customer Content; (2) and Customer Content, and Customer's end-users' use of Customer Content and Axon Cloud Services, does not violate this Policy or applicable data protection laws and regulations.

Axon may also collect, control, and process Non-Content Data. Axon is a Data Controller for Non-Content Data. Axon collects, controls, and processes Non-Content Data to provide Axon Cloud Services and to support the overall delivery of Axon Products including business, operational, and security purposes. With Non-Content Data, Axon may analyze and report anonymized and aggregated data to communicate with external and internal stakeholders. In regard to Customer Entity & User Data, Axon is a Data Controller and Customer is an independent Data Controller, not a joint Data Controller with Customer.

Data Collection and Processing Activities

CUSTOMER CONTENT

Axon will only use Customer Content to provide Customer Axon Cloud Services. Axon will not use Customer Content for any advertising or similar 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. Changes to Axon Cloud Services may increase the capabilities of the service and ways in which Customer Content can be processed.

NON-CONTENT DATA

Non-Content Data includes data, configuration, and usage information about customer's Axon Cloud Services tenant, Axon Devices, Axon Client Applications, and users that is transmitted or generated when using Axon Products. Non-Content Data includes the following:

Customer Entity And User Data

Customer Entity and User Data includes personal and non-personal data regarding Customer's Axon Cloud Services tenant configuration and users. 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 but may unsubscribe from promotional communications at any time.

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 uses 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 uses Service Operations and Security Data to provide service operations and monitoring.

Account Data

Axon uses Account Data to provide Axon Cloud Services, manage Customer's accounts, market to, and communicate with Customer. Customer may unsubscribe from promotional communications at any time.

Support Data

Axon uses Support Data to resolve Customer's support incident, and to operate, improve, and personalize Axon Products. If Customer shares Customer Content to Axon in a support scenario, the Customer Content will be treated as Support Data but will only be used for resolving support incidents.

Axon may provide support through phone, email, or online chat. With Customer's permission, Axon may use Guest Access ("GA") to temporarily navigate Customer's Axon Cloud Service's tenant to view data in order to resolve a support incident. Phone conversations, online chat sessions, or GA sessions with Axon support professionals may be recorded and/or monitored.

Server and Data Location

CUSTOMER CONTENT

Axon offers Axon Cloud Services in numerous geographic regions. Before creating an account in Axon Cloud Services, 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 & Texas, United States
CA	Canada	Microsoft Azure	Toronto, ON & Quebec City, QC
EU	European Union	Amazon Web Services	Ireland *Starting Q2 2021, new customers will not be added to this region
EUR	European Union	Microsoft Azure	Netherlands, Ireland
UK	United Kingdom	Microsoft Azure and Amazon Web Services	London, England & Cardiff, Wales
US	United States	Microsoft Azure and Amazon Web Services	Texas & Virginia, United States
US	United States (Federal Region)	Microsoft Azure	Texas & Virginia, United States
ENT	Global	Microsoft Azure	Washington & Wyoming, United States

Axon ensures that all Customer Content in Axon Cloud Services 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 is located is in the United States and may be located in Customer's selected economic area for Customer Content.

Information Sharing

Axon may transfer data with its direct and indirect subsidiaries and Sub-processors, including, without limitation, service providers and other partners to support the overall delivery of Axon Products as described in “Data Collection and Processing Activities” section of this Policy.

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.

Customer consents to the transfer of Customer Content to Axon's Sub-processors for the purpose of storing Customer Content. Such Sub-processors responsible for storing Customer Content are contracted by Axon for data storage services. Ownership of Customer Content remains with Customer.

Axon may hire Sub-processors to provide or enhance Axon Products on its behalf. Axon will only permit any such Sub-processors to obtain Customer Content from Axon Cloud Services to deliver services to Axon and will be prohibited from using Customer Content for any other purpose. Axon may engage new Sub-processors. Axon will give Customer notice (by updating the website) of any new Sub-processor.

Prior to onboarding Sub-processors, Axon conducts an audit of the security and privacy practices of Sub-processors to ensure Sub-processors provide a level of security and privacy appropriate to its access to data and scope of services.

Under Privacy Shield's “Onward Transfer Principle”, Axon remains responsible for personal data that may be shared with Axon's Sub-processors.

Customer can transfer data from Axon Cloud Services to third parties. Customer must ensure data sharing agreements are in place with third parties to protect data throughout its lifecycle.

Axon Sub-Processors

Understand the server locations, data processed, and functions performed.
Axon maintains an up-to-date list of the names and locations of all Sub-processors. This list is below.

If you are a current Axon Cloud Services customer with a data processing agreement in place with Axon, you may subscribe to receive notifications of a new Sub-processor(s) before Axon authorizes any new Sub-processor to process personal data in connection with the provision of your service.
You can subscribe to receive email notifications for changes to Axon Cloud Services Sub-processor(s) by submitting a request here.

For a complete list of Axon Sub-Processors, click here.

TELECOMMUNICATION SUB-PROCESSORS

Axon Body 3 includes embedded cellular technologies used to connect to telecommunication networks in order to provide connectivity between Axon Body 3 and Axon Cloud Services. Cellular technologies enable Axon Aware services. Customer’s Axon Body 3 cameras will send data to the respective Axon Cloud Services region selected telecommunications providers as needed to enable cellular connectivity. Data includes Personal Data, such as location data. For Axon Body 3, Axon manages all cellular

registration and account management associated to the cellular subscription. Personal Data of Customers is not collected by Axon or telecommunications providers for the purposes of cellular account management.

Outlined below is the telecommunication sub-processors. In regions where there are more than one telecommunication sub-processor, Axon will manage customers' Axon Body 3 cellular registration.

REGION CODE	ECONOMIC AREA	TELECOMMUNICATION SUB-PROCESSORS
AU	Southeast Asia	Telstra
LA	South America	TBD / TBA
CA	Canada	Telus
EU/EUR	European Union	T-Systems
UK	United Kingdom	BTEE
US	United States	Verizon and AT&T (FirstNet)
US	United States (Federal Region)	Verizon and AT&T (FirstNet)
ENT	Global	Verizon and AT&T (FirstNet)

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*

Required Disclosures

Axon will not disclose Customer Content except as compelled by a court or administrative body or required by any law or regulation. Axon will notify Customer if any disclosure request is received for Customer Content so Customer may file an objection with the court or administrative body.

Customer's Access and Choice

Customer Content

Customer can access Customer's tenant to manage Customer Content.

Non-Content Data

Within the scope of Axon's authorization to do so, and in accordance with Axon's commitment under the Privacy Shield, Axon will work with Customers to provide access to Personal Data about Customer that

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

If at any time after registering an account on Axon Cloud Services you desire to update Personal Data you have shared with us, change your mind about sharing Personal Data with us, desire to cancel your Customer account, or request that Axon no longer use provided Personal Data to provide you services, please contact us at privacy@axon.com. We will retain and use Personal Data for as long as needed to provide you services, comply with our legal obligations, resolve disputes, and enforce our agreements.

Certain data processing is determined by Customer based on Axon Product usage, Customer network or device configuration, and administrative settings made available with Axon Cloud Services or Axon Client Applications:

Axon Body 3 WiFi Positioning

Axon Body 3 cameras offer customers a feature to enhance location services where GPS/GNSS signals may not be available, for instance within buildings or underground. Customer administrators can manage their choice to use this service within the administrative features of Axon Cloud Services. When WiFi Positioning is enabled, Non-Content and Personal Data including location, device and network information data will be sent to Skyhook Holdings, Inc (Skyhook) to facilitate the WiFi Positioning functionality. Skyhook will act as both a data sub-processor (as reflected in this policy) and as a data controller. Skyhook becomes a data sub-processor for Axon when Skyhook processes data from Axon Body 3 devices to determine a location. Skyhook acts a data controller when it collects data sent from Axon Body 3 cameras to maintain their services and to develop new products, services or datasets. Data controlled by Skyhook is outside the scope of the Axon Cloud Services Privacy Policy and is subject to the Skyhook Services Privacy Policy.

Client Push Notifications

Axon Products leverage push notification services made available by mobile operating system providers (i.e. Google's Cloud Messaging and Apple's Push Notification Service to deliver functional notifications to client applications. Push notification services can be managed by leveraging notification settings made available in both mobile applications and the mobile operating system.

User Analytics

Customers can opt-out of user analytics tracking on Axon Cloud Services by disabling cookies or preventing Customer's browser or device from accepting new cookies. To prevent data from being collected by Mixpanel, network or device access to *.mixpanel.com should be blocked

Service Support

Mobile client application crash analytics are used provide Axon personnel insight to crashes when using Axon client applications. To opt out of crash reporting, network or device access to *.crashlytics.com should be blocked.

Geolocation Services

Geolocation services are critical to proper user functionality of many of Axon products. However, customers can chose to opt out of mapping and geolocation functionality by blocking network or device access to *.mapbox.com and *.arcgisonline.com

Data Security Measures

Axon is committed to help 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.

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 that Customer Data has been accessed, disclosed, altered, or destroyed by an unlawful or unauthorized party, Axon will notify relevant authorities and affected customers.

Within 48 hours of an incident confirmation, Axon will notify Customer administrators registered on Axon Cloud Services. Authorities will be notified through Axon's established channels and timelines. The notification will reasonably explain known facts, actions that have been taken, and make commitments regarding subsequent updates. Additional details are available in the Axon Cloud Services Security Incident Handling and Response Statement.

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 access to 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, may 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 Content will result in additional fees and Axon cannot warrant or guarantee data integrity or readability in the external systems.

Data Retention, Restitution, and Deletion

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 product and services and in accordance with applicable regulations. As outlined below, Customer is responsible for adhering to its own retention policies and procedures.

Evidence Retention

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. Axon Cloud Services can automate weekly messages summarizing upcoming agency-wide deletions to all customer Axon Cloud Services administrators. Customer users can receive a weekly message regarding Evidence uploaded within their user account to protect against accidental deletions. Customer can recover Evidence up to 7 days after Customer queues such Evidence for deletion. After this 7-day grace period, Axon Cloud Services initiates deletion of Evidence. Data deletion processing may occur asynchronously across storage systems and data centers. During and after data deletion processing, Evidence will not be recovered or recoverable by any party.

Accountability

As outlined herein, Axon is committed to maintaining compliance with relevant security and privacy standards to ensure the continued security, availability, integrity, confidentiality, and privacy of Axon Cloud Services and Customer Data stored within.

In addition to the security efforts outlined herein, Axon will maintain its ISO/IEC 27001:2013 certification or comparable assurances for Axon Cloud Services. Customers may review the certificate.

Social Media Publishing

Axon provides social media features that enable Customer's and their end users ("Users") to share Customer Content directly from the Evidence Detail page in Axon Evidence to social media websites ("Publish to Social Media Feature"). For example: when a User uploads a video directly to YouTube from Axon Evidence. This may include Customer Content such as video, audio, images or other types of media or multimedia; and the title, description and tags associated with those media. Customer Axon Evidence administrators can manage the enablement of this feature, for all Users, within the administrative functions of Axon Evidence. The use of this feature by Users may result in the collection or sharing of information about them, depending on the feature. The privacy and security practices of the social media website is not covered by this Policy, and Axon is not responsible for, or makes attestations regarding, their privacy or security practices. When Users enable the Publish to Social Media Feature, and/or publish content to a social media website using this feature, they acknowledge and agree to be bound by the terms of service and privacy policy(s), if applicable, of the social media website in which the Customer Content is published to. Axon encourages Users to review the terms of service and privacy policy(s) of the social media website, to make sure they understand the data that may be collected, used, and shared by the website.

- **Google LLC, (YouTube API Services)**: Axon uses YouTube's API services in connection with our Publish to Social Media Feature. When Users link, connect, or login ("Connect") their Google account(s) with Axon Evidence, they are agreeing to be bound by the YouTube Terms of Service (https://www.youtube.com/t/terms). In addition, they are directing Google to send Axon data as controlled by Google or as authorized by the User via their privacy settings at Google. Through YouTube's API services, Axon only accesses, collects, and stores a token which Axon uses to Connect the associated Google account(s) with Axon Evidence. The token is only used to enable a user to upload a video to YouTube and is not shared with external parties. Axon does not obtain or store the associated Google account(s) login credentials, through YouTube's API services.

  Google has settings that list which apps can connect to a Google account(s). When Users Connect an associated Google account(s) to Axon Evidence, Axon Evidence gets authorized in these settings as a connected site or app. If Users remove Axon Evidence from these settings, its access to the account is revoked. Users may revoke this access at any time by following the instructions here: https://help.axon.com/hc/en-us/articles/360052689392-Removing-Axon-Evidence-Access-to-Your-YouTube-Account. Revoking Axon Evidence access will prevent Users from publishing videos to YouTube from Axon Evidence.

  Axon encourages Users to review YouTube's Terms of Service (https://www.youtube.com/t/terms) and Google's Privacy Policy (http://www.google.com/policies/privacy) to make sure they understand the data that may be collected, used, and shared by Google.

Insurance

Axon will maintain, during the term of the Agreement, a cyber-insurance policy and will furnish certificates of insurance as set forth in the Master Agreement and any appendices thereto.

How to Contact Us

Axon commits to resolve complaints about Customer privacy and use of Axon Products. Complaints surrounding this Policy can be directed to Customer's local Axon representative or privacy@axon.com. If Customer has any questions or concerns regarding privacy and security of Customer Content or Axon's handling of Customer's Personal Data under Privacy Shield, please contact privacy@axon.com.

If Customer is an EU citizen and we are unable to satisfactorily resolve any complaint relating to the Privacy Shield, or if Axon fails to acknowledge Customer's complaint in a timely fashion, Customer can contact the relevant EU Data Protection Authorities (DPAs) or the Swiss Federal Data Protection and Information Commissioner (FDPIC). In certain circumstances, the Privacy Shield provides the right to invoke binding arbitration to resolve complaints not resolved by other means, as described in Annex I to the Privacy Shield Principles in each of the Privacy Shield Frameworks. Axon is subject to the investigatory and enforcement powers of the U.S. Federal Trade Commission.

Appendix A – UNIVERSITY OF NEBRASKA TECHNOLOGY
Software/Services Standardized Agreement Language

Introduction

The purpose of this document is to incorporate specific terms and conditions pertinent to technology at the University of Nebraska. This document addresses select topics of particular importance to Information Technology Services ("ITS") in order to be compliant with Board of Regents Policies, as well as Nebraska State laws.

1. INCORPORATION BY REFERENCE

This UNIVERSITY OF NEBRASKA TECHNOLOGY Software/Services Standardized Agreement Language is attached to and incorporated by reference into the Master Agreement ("Agreement") between Axon Enterprise, Inc. ("Service Provider") and the Board of Regents of the University of Nebraska as Appendix A.

2. OWNERSHIP AND PROPRIETARY RIGHTS

2.1 Service Provider owns and retains all right, title and interest in Service Provider-Owned Materials. ITS owns and retains all right, title and interest in ITS's Owned Materials. ITS Students own and retain all right, title and interest in ITS Student-Owned Material. ITS acknowledges and agrees that, unless otherwise agreed by Service Provider in writing, Service Provider is the sole and exclusive owner of all rights, including but not limited to all patent rights, copyrights, trade secrets, trademarks, and other proprietary rights in the systems, programs, specifications, user documentation, and other Service Provider-Owned Materials used by Service Provider in the course of its provision of services hereunder. ITS also acknowledges and agrees that in entering into this Agreement, ITS acquires no ownership rights in Service Provider-Owned Materials. ITS shall not copy, transfer, sell, distribute, assign, display, or otherwise make Service Provider-Owned Materials available to third parties. Service Provider acquires no rights of ownership in or to the ITS owned Materials or the Student-Owned Materials; or anything that is provided to Service Provider by ITS, including but not limited to business processes, software and related documentation. Any modifications or enhancements to the ITS Owned Materials or the Student-Owned Materials including those suggested or implemented by Service Provider, shall belong to ITS. Service Provider agrees that its rights to use any such materials or data provided by ITS, including all ITS-owned Materials is limited to such use as is necessary to permit Service Provider to perform Services and obligations in this Agreement.

2.2 ITS has the responsibility for providing Service Provider with the copyright notice language to appear on websites, delivered course content and/or assessments, and on any related practice and/or demonstration materials. Service Provider will have the responsibility for ensuring that the copyright notice language provided to Service Provider by ITS will appear as provided on any applicable materials. Any copyright notice language or other language acknowledging Service Provider's ownership or other legal rights of Service Provider which appears on websites, course content and/or assessments, and in any practice and/or demonstrational materials will be limited to such language as is necessary to protect Service Provider's legal rights. Unless provided to Service Provider by ITS, no language acknowledging the legal rights of any third party shall appear on materials without the prior written consent of ITS.

2.3 Notwithstanding anything in the Agreement to the contrary, any and all Deliverables (defined below) shall be the sole and exclusive property of ITS. Notwithstanding the foregoing, the intellectual capital (including without limitation, ideas, methodologies, processes, inventions and tools) developed or possessed by Service Provider prior to, or acquired during, the performance of the Scope of Work shall be Service Provider-Owned Material.

2.4 Upon ITS' request or upon the expiration or termination of this Agreement, Service Provider shall deliver or return all copies of the work to ITS. Service Provider is permitted, subject to its obligations of confidentiality, to retain one copy of the work for archival purposes and to defend its work product.

2.5 To the extent Service Provider develops any tangible work products identified as deliverables ("Deliverables")

solely for the use of ITS during the Term or Terms of this Agreement, Service Provider shall grant to ITS a royalty-free, worldwide, non-transferable, non-exclusive, perpetual right to use such work. Service Provider will retain all intellectual property rights and ownership in such work.

2.7 ITS recognizes that Service Provider's business depends substantially upon the accumulation of learning, knowledge, data, techniques, tools, processes, and generic materials that it utilizes and develops in its engagements. ITS's business also depends substantially upon the accumulation and application of learning, knowledge, data, techniques, tools, processes, and generic materials that it utilizes and develops through collaboration with Service Provider and other service providers. Accordingly, to the extent material that is used in, enhanced, or developed in the course of providing Services hereunder is of a general abstract character, or may be generically re-used, and does not contain Confidential Information of ITS, then Service Provider will own such material including, without limitation: methodologies; delivery strategies, approaches and practices; generic software tools, routines, and components; generic content, research and background materials; training materials; application building blocks; templates; analytical models; project tools; development tools; inventions; solutions and descriptions thereof; ideas; and know-how (collectively "Know-how") developed by Service Provider and ITS will own the Know-how developed by ITS. To the extent such Know-how is contained or reflected in the Work Product, each party hereby grants the other a fully paid up, perpetual license to use such Know-how. Neither party will sublicense or sell Know-How of the other party to any third party, and neither party will use or exploit the Know-How of the other party to compete with the information technology and professional services of Service Provider or the educational services and delivery of ITS.

3. DATA USE

As between the parties, ITS will own, or retain all of its rights in, all data and information that ITS provides to the Service Provider, as well as all data managed by Service Provider on behalf of ITS, including all output, reports, logs, analyses, and other materials relating to or generated by the Services, even if generated by the Service Provider, as well as all data obtained or extracted through ITS' or Service Provider's use of the Services (collectively, the ITS Data). The ITS Data also includes all data and information provided directly to Service Provider by ITS students and employees, and includes personal data, metadata, and user content. The ITS Data will be ITS' Intellectual Property and Service Provider will treat it as ITS' confidential and proprietary information. Service Provider will not use, access, disclose, or license or provide to third parties, any ITS Data, or materials derived therefrom, except: (i) to the extent necessary to fulfill Service Provider's obligations to ITS hereunder; (ii) as authorized in writing by ITS, and (iii) in compliance with Axon's Cloud Services Privacy Policy attached to the Agreement. Without limiting the generality of the foregoing, Service Provider may not use any ITS Data, whether or not aggregated or de-identified, for product development, marketing, profiling, benchmarking, or product demonstrations, without, in each case, ITS's prior written consent. Upon request by ITS, Service Provider will deliver, destroy, and/or make available to ITS, any or all of the ITS Data.

4. PROPRIETARY AND CONFIDENTIAL INFORMATION

4.1 Service Provider acknowledges and understands that in connection with this Agreement, the performance of the Scope of Work and otherwise, Service Provider has had or shall have access to, has obtained or shall obtain, or has been or shall be given ITS' Confidential Information (as defined herein). For purposes of this Agreement, "Confidential Information" means all information provided by ITS, or ITS students to Service Provider, including without limitation information concerning the ITS' business strategies, political and legislative affairs, students, employees, vendors, service providers, student records, customer lists, finances, properties, methods of operation, computer and telecommunications systems, software and documentation, student materials, student name and other identifying information which is generated by the student, such as biometrics. Confidential Information includes information in any and all formats and media, including without limitation oral communication, and includes the originals and any and all copies and derivatives of such information. Service Provider shall comply with all applicable federal, state and local laws restricting access, use and disclosure of protected information.

4.2 Service Provider shall use the Confidential Information only if and when required for the performance of the Services, and for no other purpose whatsoever, and only by Service Provider employees engaged in that

performance. Service Provider may also share Confidential Information with its corporate affiliates and with agents and service providers who are bound by similar obligations of confidentiality and who need such information as part of Service Provider's performance under this Agreement. Service Provider shall forward any request for disclosure of Confidential Information to:

Information Technology Services
Canfield Administration Building North (ADMN) 332
Lincoln, NE 68588-0435

4.3 Service Provider acknowledges and understands that ITS is required to protect certain Confidential Information from disclosure under applicable law, including but not limited to the Family Educational Rights and Privacy Act ("FERPA"), the Gramm Leach Bliley Act ("GLBA"), or the Nebraska Public Records Law, including regulations promulgated thereunder, as the laws and regulations may be amended from time to time. The Confidential Information that is protected under FERPA was provided to the Service Provider as it is handling an institution service or function that would ordinarily be performed by ITS' employees. Service Provider agrees that it shall be obligated to protect the Confidential Information in its possession or control in accordance with the Privacy Laws and as a "school official" under FERPA. The Service Provider further agrees that it is subject to the requirements governing the use and re-disclosure of personally identifiable information from education records as provided in FERPA.

4.4 Service Provider may disclose Confidential Information as required by legal process. If Service Provider is required by legal process to disclose Confidential Information, Service Provider shall immediately notify ITS, and before disclosing such information shall allow ITS reasonable time to take appropriate legal action to prevent disclosure of the Confidential Information.

4.5 Service Provider's obligations with respect to Confidential Information shall survive the expiration or the termination of this Agreement.

4.6 Service Provider acknowledges that its failure to comply fully with the restrictions placed upon use, disclosure and access to Confidential Information may cause ITS grievous irreparable harm and injury. Therefore, any failure to comply with the requirements of this section may be a material breach of this Agreement.

4.7 Except to the extent otherwise required by applicable law or professional standards, the obligations under this section do not apply to information that (1) is or becomes generally known to the public, other than as a result of disclosure by Service Provider, (2) had been previously possessed by Service Provider without restriction against disclosure at the time of receipt by Service Provider, (3) was independently developed by Service Provider without violation of this Agreement, or (4) Service Provider and ITS agree in writing to disclose. To the extent allowed by Nebraska State Law, each party shall be deemed to have met its nondisclosure obligations under this section as long as it exercises the same level of care to protect the other's information as it exercises to protect its own Confidential Information.

4.8 Service Provider agrees to use Student-Owned Materials, ITS Owned Materials and ITS' Confidential Information only as necessary to perform its responsibilities under this Agreement, keep it confidential in accordance with this Agreement and use reasonable commercial efforts to prevent and protect the contents of these materials, or any parts of them, from unauthorized disclosure. Further, Service Provider will take industry standard measures to protect the security and confidentiality of such information including controlled and audited access to any location where such confidential and proprietary data and materials reside while in the custody of Service Provider and employing security measures to prevent system attacks (e.g., hacker and virus attacks).

4.9 Upon termination, cancellation, expiration or other conclusion of the Agreement, Service Provider shall return all Confidential Information to ITS or, if return is not feasible, destroy any and all Confidential Information without the prior written authorization from ITS. If the Service Provider destroys the information, the Service Provider shall provide ITS with a certificate confirming the date of destruction of the data. Any data referred to

in this section that is still within Service Provider's actual or constructive control shall be subject to the terms of this Agreement in perpetuity.

4.10 ITS will implement security measures at its offices and all other associated facilities to ensure the confidentiality of Service Provider's Confidential Information and materials in manner like that provided by ITS for its own information and materials identified as confidential under this Agreement. Unless otherwise provided by separate agreement, upon termination of this Agreement, ITS shall return to Service Provider all Service Provider-Owned Materials, including software, Source Code, and/or documentation provided to ITS by Service Provider; alternatively, and at Service Provider's option, ITS shall destroy any or all of the aforementioned beyond recoverability. ITS shall not retain any electronic or other copies of any Service Provider-Owned Materials or other Service Provider Proprietary and Confidential Information absent of prior written authorization from Service Provider.

4.11 Service Provider agrees to abide by the limitation on re-disclosure of personally identifiable information (PII) from education set forth in The Family Educational Rights and Privacy Act and with the terms set forth below. 34 CFR 99.33 (a)(2) states that the officers, employees and agents of a party that receives education record information from ITS may use the information but only for the purposes for which the disclosure of the information was made. Further, Service Provider agrees to protect all ITS sensitive data including all PII, financial, corporate business intelligence or intellectual property of ITS faculty, staff, and employees in accordance with generally accepted Information security standards and best practices.

5. INTENTIONALLY OMITTED

6. TERMINATION

6.1 The University may terminate this Agreement upon thirty (30) days' written notice in accordance with the terms of the Agreement.

6.2 The University may terminate this Agreement upon any breach by Service Provider of the terms of this Agreement, any Business Associate Addendum, or incorporated attachment to the Agreement, in accordance with the terms of the Agreement.

6.3 Service Provider may terminate this Agreement if the University materially breaches this Agreement and then fails to correct such breach within thirty (30) days following receipt of written notice from Service Provider. In the event of an uncorrected breach by the University, the Service Provider shall be entitled to recover actual amounts owed by the University to Service Provider that accrued on or before the date of termination. Service Provider expressly waives and disclaims any right or remedy it may have to unilaterally de-install, disable or repossess any Software of any portion thereof.

6.4 The University's rights to the Software as provided in this Agreement will survive a bankruptcy claim by the Service Provider consistent with applicable laws. The rights granted under this Agreement shall be deemed a license of "intellectual property" for purposes of the United States Code, Title 11 ("Bankruptcy Code"), Section 365(n). In the event of the bankruptcy of Service Provider and a subsequent rejection of this Agreement, the University may elect to retain its license rights, subject to and in accordance with the provisions of the Bankruptcy Code or other applicable law.

6.5 The following Sections shall survive the expiration or termination of this Agreement: Grant of License; Ownership and Proprietary Rights; Warranties, Representations and covenants; Limitation of Liability; University Data; Privacy; Cyber Insurance; Termination; and Audit Rights. Any terms of this Agreement which by their nature extend beyond its termination remain in effect until fulfilled and apply to respective successors and assigns.

7. SECURITY

7.1 Service Provider will implement security measures at its offices and all other associated facilities in connection with Service Provider software to ensure the strictest confidentiality of ITS' Owned Materials, ITS' Confidential Information, and all other confidential information and materials. These measures will include, without limitation, encryption, use of a sign-on and access privilege system and other measures described in this Agreement, and such other measures as Service Provider deems necessary in its professional discretion. Service Provider shall impose these measures on all subcontractors used by Service Provider.

7.2 Service Provider shall endorse ITS' requirement to adhere to the University of Nebraska's (ITS) IT Security Standards (http://idm.unl.edu/authentication-services-policy). ITS is required to assess risks, ensure data integrity, and determine the level of accessibility that must be maintained. Specific activities include:

A. Identification of security, privacy, legal, and other organizational requirements for recovery of institutional resources such as data, software, hardware, configurations, and licenses at the termination of the contract.
B. Assessment of the Service Provider's security and privacy controls.
C. Including ITS' security and privacy requirements in the agreement.
D. Periodic reassessment of Service Provider services provisioned to ensure all contract obligations are being met and to manage and mitigate risk.

7.3 Service Provider shall (i) establish and maintain industry standard technical and organizational measures to help to protect against accidental damage to, or destruction, loss, or alteration of the materials; (ii) establish and maintain industry standard technical and organizational measures to help to protect against unauthorized access to the Services and materials; and (iii) establish and maintain network and internet security procedures, protocols, security gateways and firewalls with respect to the Services. Service Provider software and its components are equipped and/or designed with systems intended to prevent industry known system attacks (e.g., hacker and virus attacks) and unauthorized access to Confidential Information.

7.4 For the purposes of this article, a "Breach" has the meaning given to it under relevant Nebraska or federal law, for example; the Nebraska Financial Data Protection and Consumer Notification of Data Security Breach Act of 2006 (codified at Neb. Rev. Stat. § 87-802) (See 9.5). Service Provider's report shall identify: (i) the nature of the unauthorized use or disclosure, (ii) the CDI used or disclosed, (iii) the identity of the individual or entity that received the unauthorized disclosure, (iv) any pertinent application, access, or security logs or analysis (v) the action(s) that the Service Provider has taken or shall take to mitigate any potentially negative effects of the unauthorized use or disclosure, and (vi) the corrective action(s) the Service Provider has taken or shall take to prevent future similar unauthorized uses or disclosures. Service Provider shall provide additional information in connection with the unauthorized disclosure reasonably requested by ITS.

In the event of a breach arising out of Service Providers negligence or misconduct, Service Provider agrees to promptly reimburse all costs to ITS arising from such breach, including but not limited to (i) costs of notification of individuals, (ii) credit monitoring and/or identity restoration services, (iii) time of ITS personnel responding to the breach, (iv) civil or criminal penalties levied against ITS, attorneys' fees, court costs, etc.

7.5 The contact for the ITS Computer Incident Response Team (CIRT) shall be identified as: 402-472-5700 or its-sec@nebraska.edu. Report any confirmed or suspected breach of University data to ITS's CIRT within forty-eight (48) hours of discovery or detection.

7.6 ITS or an appointed audit firm (Auditors) has the right to audit Service Provider. Audits will be at ITS' sole expense which includes operational charges by Service Provider, except where the audit reveals material noncompliance with contract specifications, in which case the cost, inclusive of operational charges by Service Provider, will be borne by the Service Provider. In lieu of ITS or its appointed audit firm performing their own audit, if Service Provider has an external audit firm that performs a review, ITS has the right to review the controls tested as well as the results and has the right to request additional controls to be added to the certified report for testing the controls that have an impact on ITS data.

7.7 Service Provider will, prior to the Agreement effective date and annually thereafter during the Term (as well as promptly after any Security Breach), engage an independent CPA firm to conduct a review of controls

over security, availability, processing integrity, confidentiality and privacy related to the Service Provider's information technology system. Such review will be conducted at the Service Provider's expense and in accordance with the AICPA's Statements on Standards for Attestation Engagements No. 16 ("SSAE") Service Organization Controls Type 1 or Type 2 report (SOC 1/SOC 2). Service Provider will provide ITS with a copy of the SOC report within thirty (30) days of the ITS' request. If exceptions are noted in the SOC audit, Service Provider will document a plan to promptly address such exceptions and will implement corrective measures within a reasonable period. Service Provider will provide a copy or summary of the exception remediation plan within thirty (30) days of ITS' request and keep ITS informed of the progress and completion of corrective measures. If a SOC audit has not been conducted in the past twelve (12) months and Service Provider is unable to provide associated SOC reports, at ITS' request, Service Provider will appoint a qualified CPA firm to conduct a SOC audit and shall provide ITS with a copy of each applicable SOC report at Service Provider's expense. To the extent the SOC reports provided to ITS do not satisfy ITS' reporting or audit requirements, ITS may conduct its own audits at its expense.

7.8 The Federal Trade Commission has promulgated regulations collectively known as the "Red Flags Rule" with which ITS must comply. See 16 CFR 681. Under the Red Flags Rule, ITS must ensure that Service Provider either complies with ITS' identity theft Program or that Service Provider has its own policies and procedures in place to detect and respond to identity theft Red Flags. Service Provider represents and warrants that is has reasonable policies and procedures in place to detect, prevent and mitigate identity theft. Service Provider shall review and comply with all relevant portions of ITS' identity theft policy, if any, as well as any applicable ITS identity theft plan. Service Provider shall report any Red Flags that it detects in connection with the Agreement to ITS.

8. CYBER INSURANCE

The Service Provider agrees to purchase and maintain throughout the term of this Agreement a technology/professional liability insurance policy, including coverage for network security/data protection liability insurance (also called "cyber liability"), covering liabilities for financial loss resulting or arising from acts, errors, or omissions in rendering technology/professional services or in connection with the specific services described in violation or infringement of any right of privacy, including: breach of security and breach of security/privacy laws, rules or regulations globally, now or hereinafter constituted or amended; data theft, damage, unauthorized disclosure, destruction, or corruption, including without limitation, unauthorized access, unauthorized use, identity theft, theft of personally identifiable information or confidential corporate information in whatever form, transmission of a computer virus or other type of malicious code, and participation in a denial of service attack on third party computer systems; loss or denial of service; no cyber terrorism exclusion, with a minimum limit of $10,000,000 each and every claim and in the aggregate. Such coverage must include technology/professional liability including breach of contract, privacy and security liability, privacy regulatory defense and payment of civil fines, payment of credit card provider penalties, and breach response costs (including without limitation, notification costs, forensics, credit protection services, call center services, identity theft protection services, and crisis management/public relations services).

Such insurance must explicitly address all of the foregoing without limitation if caused by an employee of the Service Provider or an independent contractor working on behalf of the Service Provider in performing services under this Agreement. The policy must provide coverage for wrongful acts, claims, and lawsuits anywhere in the world. Such insurance must include affirmative contractual liability coverage for the data breach indemnity in this Agreement for all damages, defense costs, privacy regulatory civil fines and penalties, and reasonable and necessary data breach notification, forensics, credit protection services, public relations/crisis management, and other data breach mitigation services resulting from a confidentiality or breach of security by or on behalf of the Service Provider.

9. MISCELLANEOUS TERMS

9.1 Accessibility **(**Section 508 ADAA Compliance). If the solution includes any end-user-facing human interface, such as an end-user device software component or web site form, file upload system, etc., then the Service Provider shall conform with the Web Content Accessibility Guidelines (WCAG) 2.1 Level AA Success Criteria to the greatest extent possible.. The Service Provider further agrees to indemnify and hold harmless the

University of Nebraska campuses and system using the Service Provider's products or services from any third party claim arising out of its failure to comply with the aforesaid requirements.

ITS, at its discretion, may at any time test the Service Provider's products or services covered by this Agreement to ensure compliance with the requirements set forth above. If ITS has any accessibility issues, then ITS must contact it's designated Service Provider representative or accessibility@axon.com and identify the particular accessibility issue(s) with as much specificity as possible. If an accommodation is found to be necessary due to a verified accessibility issue, then Service Provider agrees to remediate the accessibility issue upon request or provide an alternative accommodation at Service Provider's cost. If the accessibility issue cannot be immediately remediated, then Axon will provide a reasonable timeline for any requested remediation or accommodation. Service Provider agrees that, upon ITS's written request, Service Provider will provide updates or reports to ITS regarding Service Provider's progress with respect to any requested remediation or accommodation. Testing that results discovery of a verified accessibility issue may, in ITS's sole discretion, result in payments for impacted products or services under the Agreement being withheld. All withheld amounts will be paid to the Service Provider upon correction of the non-compliance and acceptance by ITS. Said acceptance will not be unreasonably withheld.

Failure to comply with these requirements shall constitute a breach and be grounds for termination of this Agreement and a pro-rated refund of fees paid from ITS for the remainder of original contract period.
The parties agree that a verified accessibility issue will not include issues due to intermediary interference (e.g. virus protection software, outdated web browsers or outdated assistive technology) or a user's inability to properly utilize compliant assistive technology. Client agrees to cooperate and work with Axon to discuss options for accessibility and accommodations. If the parties cannot agree that there is a verifiable accessibility issue, then Axon reserves the right to consult with an independent and mutually agreeable accessibility expert to verify the accessibility issue, provide remediation options and/or provide an alternative accommodation. Such right shall not affect University's right to withhold payment set forth above. To the extent that Axon utilizes other third-party applications or plug-ins, now or in the future, Axon encourages third-parties to make their products and services accessible. These third-party applications and/or plug-ins are not controlled by Axon and may present challenges for individuals with disabilities that Axon may not be able to control or remedy.

9.2 **University & State College Participation.** In some instances, state colleges or state agencies may wish to explore the possibility of sharing in the benefits of this contract.

9.3 **Examination of Records.** ITS shall have access to and the right to examine any pertinent books, documents, papers, and electronic records such as logs of the Service Provider involving transactions and work related to this Agreement. Service Provider shall retain project records for a period of three (3) years from the date of final payment.

9.4 **Assistance with Litigation or Investigation.** E-Discovery: In order to provide ITS with the ability to be compliant with e-discovery rules, Service Provider must provide the following where "relevant data" might include any data stored regarding any person affiliated with ITS, access logs, activity logs, transaction logs, changes to access rights, etc., as detailed by the system architecture and practices provided by Service Provider.

The rest of this page is left intentionally blank.

For the Board of Regents of the University of Nebraska

Signature: Chris Kabourek Date: 12/21/22 | 12:48 CST

Printed Name: Chris Kabourek

Title: Senior VP | CFO

For the Service Provider (Service Provider)

Signature: Robert E Driscoll Date: 12/16/2022 | 12:06 PM MST

55DAEBB131A4424...

Printed Name: Robert E Driscoll

Title: VP, Assoc. General Counsel

I affirm that if I am an employee of the University of Nebraska, I have notified buyer of my status as such and that this contract must be completed in accordance with Board of Regents Policy 6.2.1.12, Purchases involving University Personnel.

Notice. Any notice to either party hereunder shall be in writing and shall be served either personally or by registered or certified mail addressed to the following individuals:

To the Service Provider:

Axon Enterprise, Inc.
17800 N 85th Street
Scottsdale, AZ 85255
Attn: General Counsel

To the University:

Legal Notices
C/O P2P Procurement Contracts
1700 Y Street, BSC 125
Lincoln, NE 68588-0645

Part 1 – Axon Evidence Service Level Agreement

This Service Level Agreement (**SLA**) identifies the Axon Evidence Service Offerings and the expected level of services between Axon[1] (**Axon, us** or **we**) and users of Service Offerings (**Customer** or **you**). Unless otherwise provided in this SLA, this SLA is subject to the terms of the purchase agreement, or other similar agreement, if any, between Axon and Customer. This SLA applies separately to each Customer using Service Offerings. By using Service Offerings, you agree that you understand this SLA and you accept and agree to be bound by the following terms and conditions. Axon reserves the right to update and change the terms of this SLA. When we post changes, we will revise the "last updated" date at the top of this page. If there are adverse material changes to this SLA, we will inform you by directly sending you a notification. We encourage you to periodically review the most current version of the Axon Cloud Services Maintenance Schedule by visiting: https://www.axon.com/products/axon-evidence/maintenance-schedule.

Definitions

- **"Axon Cloud Services"** means Axon's web services for Axon Evidence, Axon Records, Axon Dispatch, and interactions between Evidence.com and Axon devices or Axon client software. Axon Cloud Service excludes third-party applications, hardware warranties, and my.evidence.com.
- **"Downtime"** means periods of time, measured in minutes, in which the Service Offering is Unavailable to you. "Downtime" does not include Scheduled Downtime and does not include Unavailability of the Service Offering due to limitations described under the section Exclusions.
- **"Incident"** means a disruption of Service Offerings during which the Customer experiences Downtime.
- **"Maximum Available Minutes"** means the total amount of accumulated minutes during a Service Month for the Service Offering.
- **"Monthly Uptime Percentage"** means (Maximum Available Minutes - Downtime) / Maximum Available Minutes * 100.
- **"Scheduled Downtime"** means periods of time, measured in minutes, in which the Service Offering is unavailable to Customer, which fall within scheduled routine maintenance or planned maintenance timeframes.
- **"Service Month"** means a calendar month at Coordinated Universal Time (UTC).

[1] "Axon" refers to the Axon entity that you are in a contractual agreement with for the provision of Axon Cloud Services, including but not limited to Axon Public Safety UK Limited, Axon Public Safety Germany SE, etc.

- **"Service Credits"** means credits received by users of Service Offerings in the event that the service level objectives are not achieved.
- **"Service Offerings"** means all Axon Evidence services provided by Axon pursuant to this SLA.
- **"Unavailable"** and **"Unavailability"** means a situation where the Service Offering does not allow for the upload of evidence files, viewing of evidence files or interactive login by an end-user.

Service Level Objective

Axon will use commercially reasonable efforts to make the Service Offerings available 99.99% of the time. Guaranteed service level & Service Credits:

Monthly Uptime Percentage	Service Credit in Days
Less than 99.9%	3
Less than 99.0%	7

Requesting Service Credits

In order for Axon to consider a claim for Service Credits, you must submit the claim to Axon Customer Support (https://www.axon.com/contact) including all information necessary for us to validate the claim, including but not limited to: (i) a detailed description of the Incident; (ii) information regarding the time and duration of the Incident; (iii) the number and location(s) of affected users (if applicable); and (iv) descriptions of your attempts to resolve the Incident at the time of occurrence.

Service Maintenance

- Maintenance will take place according to the prevailing Axon Cloud Services Maintenance Schedule: https://www.axon.com/products/axon-evidence/maintenance-schedule.
- Maintenance periods may periodically result in the Service Offerings being Unavailable to you. Downtime falling within scheduled routine or planned maintenance is Scheduled Downtime and is not eligible for Service Credits.
- Emergency maintenance may have less than a 24-hour notification period. Emergency maintenance may be performed at any time, with or without notice as deemed necessary by Axon. Emergency maintenance falling outside scheduled routine or planned maintenance is eligible for Service Credits.
- Axon will make available updates as released by Axon to the Axon Cloud Services. The Customer is responsible for maintaining the computer equipment and internet connections necessary for use of Axon Cloud Services.

- For the support of Android & iOS Applications, including Axon View, Axon Device Manager, and Axon Capture, Axon will use reasonable efforts to continue supporting previous version of such applications for 45 days after the change. In the event the Customer does not update their Android/iOS application to the most current version within 45 days of release, Axon may disable the application or force updates to the non-supported application.

Terms

Axon must receive the claim within one month of the end of the month in which the Incident that is the subject of the claim occurred. For example, if the Incident occurred on February 12th, we must receive the claim and all required information by March 31st.

We will evaluate all information reasonably available to us and make a good faith determination of whether a Service Credit is owed. We will use commercially reasonable efforts to process claims during the subsequent month and within forty-five days of receipt. You must be in compliance with all Axon agreements in order to be eligible for a Service Credit. If we determine that a Service Credit is owed to you, we will apply the Service Credit to the end of your Service Offering subscription term. Service Credits may not be exchanged for or converted to monetary amounts.

Exclusions

This SLA does not apply to any unavailability, suspension or termination of the Service Offerings, or any other Axon Evidence performance issues: (a) caused by factors outside of our reasonable control, including any force majeure event, terrorism, sabotage, virus attack or Customer internet access and related problems beyond the demarcation point of the Service Offerings (including Domain Name Server issues outside our direct control); (b) that result from any actions or inactions of you or a third party; (c) that result from your communication delays, including wrong, bad or missing data, improperly formatted, organized or transmitted data received from you, or any other data issues related to the communication or data received from or through you; (d) that result from your equipment, software or other technology and/or third party equipment, software or other technology (other than third party equipment within our direct control); (e) that result from any maintenance as provided for pursuant to this SLA; or (f) arising from our suspension and termination of your right to use the Service Offerings in accordance with the agreement for the provision of Axon Evidence between you and Axon.

Planned Maintenance

Axon may schedule and plan maintenance windows outside of the timeframes detailed in “Scheduled Routine Maintenance”.

Scheduled Routine Maintenance: routine maintenance is scheduled on the fourth Tuesday of each month in Pacific Time (PT)*:

DEPLOYMENT	DAY OF WEEK (PT)	PACIFIC TIME (PT)*	COORDINATED UNIVERSAL TIME (UTC)
Australia**	Tuesday	02:00 - 05:00	10:00 - 12:00
Brazil	Tuesday	10:00 - 11:00	17:00 - 19:00
European Union	Tuesday	13:00 - 14:00	20:00 - 22:00
United Kingdom**	Tuesday	14:00 - 15:00	21:00 - 23:00
Canada	Tuesday	16:00 - 17:00	23:00 - 01:00***
United States - Federal Region	Tuesday	17:00 - 18:00	00:00 - 02:00****
United States	Tuesday	21:00 - 22:00	04:00 - 06:00****

* Pacific Time (PT) observes daylight savings. UTC time data is reflective of maintenance windows regardless of daylight savings observation. Refer to UTC to calculate local time of maintenance.
** Maintenance performed on UK and AU a week after the fourth Tuesday of each month
*** Time period includes time on Wednesday in UTC
**** Time period is on Wednesday in UTC

Emergency Maintenance

Patches and emergency releases are used to deliver ad-hoc application fixes and are typically seamless to customers. Whenever possible, patches and emergency releases are deployed during off-peak hours and without Downtime. Emergency releases are conducted on an as-needed basis and can occur any day of the week.

Axon Device Firmware Updates

Firmware updates and enhancements to Axon devices are pushed from Axon Cloud Services. Customer interaction is not required. Updates are retrieved, installed and validated during the normal device charging and data transfer process. Firmware updates are systemically rolled out to customers in waves.

Notification of Maintenance

Notification of upcoming routine maintenance is not provided in advance unless there has been a change to the Scheduled Routine Maintenance. Approximately one (1) week prior to the routine maintenance, release notes are provided to Axon Evidence customer administrators.

If planned maintenance is required, Axon will communicate via email to Axon Evidence Customer administrators at least one (1) week in advance.

In the event of scheduled routine or planned maintenance that requires customer action (e.g. updating network settings), Axon will communicate via email at least sixty (60) days prior to the maintenance. Please Note: If emergency maintenance that requires customer action is necessary, Customers may be notified less than one (1) week in advance.

Part 2 - Customer Support Response Statement

Axon has implemented Incident response policies and practices for Axon devices and Axon Cloud Services, which follow industry best practice standards. Axon reserves the right to change the terms of these response policies.

Definitions

- "**Business Day**" means Monday to Friday 08:00 – 17:30, excluding public holidays.
- "**BOD**" means the Board of Directors
- **"Incident"** means a fault related to an Axon product or Axon Cloud Services experienced by the Customer.
- **"Targeted Response Time"** means the target timeframe for Axon to respond to Customer and/or escalate the Incident within the "*Axon Customer Support Solution".*
- **"Targeted Resolution Time"** means the target timeframe for the full resolution of the Incident. It excludes time delays caused by Customer or third parties outside of Axon's reasonable control.
- "**Workaround**" means a method for overcoming an Incident allowing the Customer to operate the core function of Axon devices and/or Axon Cloud Services.

Axon Support Channels

Axon Resource Centre: https://my.axon.com

Telephone:

US & Canada: 800-978-2737
UK: +44 (0)1327 709 666

Email:

UK: uksupport@axon.com
Germany: support-dach@axon.com
Rest of EMEA: customerservice@axon.com or support@axon.com

Incident Classifications and Response Times

Incident Classification	Description	Targeted Response Time	Targeted Resolution Time	Customer Response Commitment
Severity 1	- Business critical function is down - Material impact to Customer's business - No Workaround exists	Less than 1 hour	Less than 24 hours	Customer shall remain accessible by phone for troubleshooting from the time a Severity 1 issue is logged until such time as it is resolved.
Severity 2	- Business critical function is impaired or degraded - There are time-sensitive issues that materially impact ongoing production - Workaround exists, but it is only temporary	1 Business Day	Less than 2 weeks	Customer shall remain accessible by phone or other electronic means for troubleshooting from the time a Severity 2 issue is logged until such time as it is resolved.
Severity 3	- Non-critical function down or impaired - Does not have significant current production impact - Performance is degraded	1 Business Day	Mutually agreed timeframe based on prioritization	

For Customers with 4 levels of Incident classification such as Critical, High, Medium and Low, Axon will recognize this and will consider the two highest categories as “Severity 1”. For example: Critical and High would be classed as a “Severity 1” Incident and managed accordingly.

Severity Level Determination

Customer shall reasonably self-diagnose each Incident and recommend to Axon an appropriate severity level designation. Axon shall validate your severity level designation or notify you of a proposed change to a higher or lower level with justification for the proposal. In the event of a conflict regarding the appropriate severity level designation, each party shall promptly escalate such conflict to its management team for resolution through consultation between the parties’ management, during which time the parties shall continue to handle the Incident support in accordance with Axon’s severity level designation. In the rare case a conflict requires a management discussion, both parties shall be available within one hour of the escalation.

Escalation

Escalation Level	Description	Escalation	Targeted Response Time	Targeted Resolution Time
Tier 1	**Basic technical or commercial issues - Non-time critical**	None	Less than 6 hours	Less than 1 business day
Tier 2	**Advanced technical or commercial issues - Non-time critical.**	BoD / Country Manager	Less than 4 hours	Less than 1 business day
Tier 3	**Technical or commercial issues - Time critical**	Country Manager to Axon BoD/Support Team	Less than 2 hours	Less than 1 business day

Exclusions

This Customer Support Response Statement does not apply to any unavailability, suspension, or termination of the Service Offerings caused by all the exclusion events under Part 1 of this document, nor to services or hardware not within Axon's control. Hardware warranty will be dependent on Customer's specific agreement with Axon and levels covered. Please see Part 3 for "Return of Merchandise Authorization".

Part 3 – Return of Merchandise Authorization (RMA)

The *Axon Evidence Device Return Service* provides Customers with the ability to manage return merchandise authorization (RMA) requests within Axon Evidence.com. Authorized users will be able to create, update, save, submit, and track device returns for their agency in one place. Hardware warranty will be dependent on Customer's specific agreement with Axon and levels covered.

Targeted Replacement Time:

Axon aims to have replacement devices shipped to the Customer within 48 hours from receipt of the faulty device (excluding weekends or public holidays).

Exclusions

The Return of Merchandise Authorization does not apply to services or hardware not within Axon's control. Axon's customer support will provide detail on return times as soon as possible to the Customer's point of contact.

N.B. *TASER products (conducted electrical devices) are not covered under the terms of this Return of Merchandise Authorization. Customers are requested to contact Customer support directly to report a faulty TASER device.*

BUSINESS ASSOCIATE AGREEMENT

This Business Associate Agreement (this "Agreement") is entered into by and between Axon Enterprise, Inc., a Delaware corporation with an address located at 17800 N 85th Street, Scottsdale, AZ 85255 (herein referred to as "Business Associate"), and The Board of Regents of the University of Nebraska, a public body corporate,(herein referred to as "Covered Entity") and shall be effective on the later of the dates of the parties' signatures below (the "Effective Date").

1. **Definitions**.

1.1. "HIPAA Regulations" means the Administrative Simplification requirements of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), and the regulations promulgated thereunder, including (i) the Standards for Privacy of Individually Identifiable Health Information at 45 C.F.R. Parts 160 and 164 (Subparts A and E) (the "HIPAA Privacy Rule"); (ii) the Administrative Requirements applicable to Transactions at 45 C.F.R. Parts 160 and 162 (Subparts A and I) (the "Electronic Transactions Rule"); (iii) the Security Standards for the Protection of Electronic Protected Health Information at 45 C.F.R. Parts 160 and 164 (Subparts A and C) (the "HIPAA Security Rule"); and (iv) the Standards for Notification in the Case of Breach of Unsecured Protected Health Information at 45 C.F.R. Parts 160 and 164 (Subparts A and D).

1.2. "HITECH Act" means the Health Information Technology for Economic and Clinical Health Act, Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (Pub. L. 111-5).

1.3. "Protected Health Information" or "PHI" means information, including demographic information, that (i) relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual; (ii) identifies the individual (or there is a reasonable basis for believing that the information can be used to identify the individual); and (iii) is received by Business Associate from or on behalf of Covered Entity, is created by Business Associate on behalf of Covered Entity, or is made accessible to Business Associate by Covered Entity.

1.4. "Services" means provision of Axon Cloud Services as described in the agreement between the Parties (the "Underlying Agreement").

1.5. "Successful Security Incident" shall mean a Security Incident that results in the unauthorized access, use, disclosure, modification, or destruction of PHI.

1.6. "Unsuccessful Security Incident" shall mean a Security Incident that does not result in unauthorized access, use, disclosure, modification, or destruction of PHI (including, for example, and not for limitation, pings on Business Associate's firewall, port scans, attempts to log onto a system or enter a database with an invalid password or username, denial-of-service attacks that do not result in the system being taken off-line, or malware such as worms or viruses).

1.7. Except as otherwise set forth in this Agreement, capitalized terms used, but not otherwise defined, in this Agreement shall have the same meanings as those terms in the HIPAA Regulations. A reference in this Agreement to the HIPAA Regulations, the HIPAA Privacy Rule, the Electronic Transaction Rule, the HIPAA Security Rule and the HITECH Act

means the law or regulation as may be amended from time to time. Any ambiguity in this Agreement shall be resolved to permit compliance with the HIPAA Regulations.

2. **Business Associate's Satisfactory Assurances**.

2.1. *Permitted Uses of PHI.* Business Associate shall Use PHI only as necessary to perform the Services, for Business Associate's proper management and administration, or to carry out Business Associate's legal responsibilities. If and only to the extent part of the Services, Business Associate may perform data aggregation with regard to the health care operations of Covered Entity.

2.2. *Permitted Disclosures of PHI.* Business Associate shall Disclose PHI only:

2.2.1. As necessary to perform the Services;

2.2.2. For Business Associate's proper management and administration or to carry out Business Associate's legal responsibilities, provided that:

2.2.2.1. The Disclosure is Required By Law; provided, however, that Business Associate shall notify Covered Entity no less than five (5) business days prior to any such Disclosure and provide Covered Entity with the opportunity to seek confidential treatment for any PHI Disclosed and cooperate with Covered Entity if it should seek confidential treatment; or

2.2.2.2. Prior to the Disclosure, Business Associate obtains reasonable written assurances from the person or entity to whom the PHI is Disclosed that:

(a) the PHI will be held in confidence and Used or further Disclosed only as Required By Law or for the lawful purpose for which it was Disclosed to the person or entity; and

(b) the person or entity will notify Business Associate of any instances of which it is aware in which the confidentiality of the PHI has been breached within two (2) days of becoming aware of such an occurrence.

2.3. *Confidentiality Obligation.* Business Associate will not Use or Disclose PHI other than as permitted by this Agreement or as Required By Law.

2.4. *Safeguards.* Business Associate agrees to implement appropriate administrative, physical, and technical safeguards to prevent the unauthorized Use and Disclosure of Protected Health Information, and to protect the confidentiality, integrity, and availability of Electronic Protected Health Information, as required by the HIPAA Regulations. Without limiting the foregoing, Business Associate agrees to comply with the requirements of the HIPAA Security Rule.

2.5. *Deidentification*. Business Associate may not de-identify Protected Health Information except as necessary to provide the Services. Business Associate is prohibited from Using or Disclosing any such deidentified information for its own purposes without the prior

written consent of Covered Entity. Business Associate is further prohibited from Disclosing such deidentified information to any third party who may reidentify such information, in violation of 45 C.F.R. 164. Such disclosure shall constitute a breach of this Agreement.

2.6. *Access.* If and to the extent Business Associate maintains PHI in a Designated Record Set, Business Associate shall make the PHI specified by Covered Entity available to the individual(s) identified by Covered Entity as being entitled to access in accordance with 45 C.F.R. § 164.524, as amended by the HITECH Act. If Covered Entity determines that an Individual is entitled to such access, and that such PHI is under the control of Business Associate, Covered Entity will communicate the decision to Business Associate. Covered Entity shall provide access to the PHI in the same manner as would be required for Covered Entity. If Business Associate receives an Individual's request to access his or her PHI, Business Associate shall forward such request to Covered Entity within five (5) business days.

2.7. *Amendment.* Upon request by an Individual, Covered Entity shall determine whether any Individual is entitled to amend his or her PHI pursuant to 45 C.F.R. § 164.526. If Covered Entity determines that an Individual is entitled to such an amendment, and that such PHI is both in a Designated Record Set and under the control of Business Associate, Covered Entity will communicate the decision to Business Associate. Business Associate shall provide an opportunity to amend the PHI in the same manner as would be required for Covered Entity. If Business Associate receives an Individual's request to amend his or her PHI, Business Associate shall forward such request to Covered Entity within five (5) business days.

2.8. *Accounting.* Upon Covered Entity's request, Business Associate shall make available to Covered Entity the information necessary to provide an accounting of each Disclosure of PHI made by Business Associate in accordance with 45 C.F.R. § 164.528. If Business Associate receives an Individual's request for an accounting of Disclosures, Business Associate shall forward such request to Covered Entity within five (5) business days and will thereafter follow the directions of Covered Entity with respect to such a request for an accounting.

2.9. *Restrictions on Disclosures.* Upon request by an Individual, Covered Entity shall determine whether an Individual is entitled to a restriction on disclosure of PHI pursuant to 45 C.F.R. § 164.522. If Covered Entity determines that an Individual is entitled to such a restriction, Covered Entity will communicate the decision to Business Associate. Business Associate will restrict its Disclosures of the Individual's PHI in the same manner as would be required for Covered Entity. If Business Associate receives an Individual's request for a restriction, Business Associate shall forward such request to Covered Entity within five (5) business days.

2.10. *Activities to Assist Covered Entity's Compliance with the HIPAA Privacy Rule.* In the event the performance of the Services requires Business Associate to perform any activity on behalf of Covered Entity in order to assist Covered Entity in complying with the HIPAA Privacy Rule, Business Associate agrees to comply with the requirements of the HIPAA Privacy Rule that apply to Covered Entity in the performance of such activity.

2.11. *Access to Books and Records.* Business Associate shall make its internal practices, books and records relating to the Use and Disclosure of PHI available to the Secretary for purposes of determining compliance with the HIPAA Regulations.

2.12. *Background Screenings*. Business Associate has obtained, at Business Associate's own expense and in a manner compliant with all applicable local, state, federal and international laws, including the Federal Bureau of Investigation Criminal Justice Information Services Security Addendum, a background screening for all of its Workforce members with access to any Protected Health Information, which background screening was completed consistent with current industry standards and included, without limitation, a national federal criminal database check, a seven (7) year county of residence criminal conviction search, and, as applicable, an international criminal record check (a "Satisfactory Background Screening"). If additional Workforce members (whether existing or new hires) will have access to any Protected Health Information, Business Associate shall ensure Business Associate has obtained a Satisfactory Background Screening for each such additional Workforce member prior to permitting him/her any access to Protected Health Information. Business Associate agrees to update any Workforce background screening upon reasonable request by Covered Entity, it being agreed that any request based upon the occurrence of any Breach or other illegal activity involving Business Associate or its personnel, or the reasonable suspicion of illegal activity involving Protected Health Information, or any regulatory requirements requiring such updates, would be deemed reasonable hereunder. Business Associate shall provide Covered Entity with evidence of the completion of the required Satisfactory Background Screenings upon Covered Entity's request. Business Associate shall not hire, retain or engage any Workforce who will have access to any PHI who has been convicted (felony or misdemeanor) of or entered into a court-supervised diversion program for theft or fraud (including, but not limited to, embezzlement, larceny, perjury, forgery, credit card fraud, check fraud, identity theft), terrorism, or any other breach of trust or fiduciary duty crime.

2.13. *Agents and Subcontractors.* Business Associate shall not permit any agent, Subcontractor or other third party to create, access, receive, maintain, transmit, use, disclose or store PHI in any form on behalf of Business Associate without Covered Entity's prior written consent. Business Associate agrees to ensure that any permitted agent or permitted Subcontractor to which it provides Protected Health Information agrees to the same requirements that apply through this Agreement to Business Associate with respect to such information and to enter into a written business associate agreement with any such agent or Subcontractor. Business Associate shall be liable to Covered Entity for any acts, failures or omissions of the agent or Subcontractor in providing the services as if they were Business Associate's own acts failures or omissions to the extent permitted by law.

2.14. *Reporting of Violations.* Business Associate shall report to Covered Entity any of the following events within two (2) business days of becoming aware of the occurrence of the event:

2.14.1. Any Use or Disclosure of PHI not authorized by this Agreement;

2.14.2. Any Successful Security Incident; and

2.14.3. Any acquisition, access, Use or Disclosure of Unsecured PHI in a manner not permitted by the HIPAA Privacy Rule. Such report shall include the identification of each Individual whose Unsecured PHI has been, or is reasonably believed by

Business Associate to have been, accessed, acquired, Used or Disclosed. As soon as possible thereafter, and to the extent known, Business Associate shall also provide Covered Entity with a description of:

2.14.3.1. What happened, including the date of the acquisition, access, Use or Disclosure and the date of its discovery;

2.14.3.2. The types of Unsecured PHI involved in the acquisition, access, Use or Disclosure;

2.14.3.3. Any steps Individuals should take to protect themselves from potential harm from the acquisition, access, Use or Disclosure; and

2.14.3.4. What Business Associate is doing to investigate the acquisition, access, Use or Disclosure, to mitigate harm to Individuals, and to protect against any further unpermitted acquisition, access, Use or Disclosure of Unsecured PHI.

2.15. *Reporting Unsuccessful Security Incidents.* The Parties acknowledge and agree that this Section constitutes notice by Business Associate to Covered Entity of the ongoing existence and occurrence of Unsuccessful Security Incidents. The foregoing notwithstanding, Business Associate shall, upon Covered Entity's reasonable written request, report to Covered Entity Unsuccessful Security Incidents in accordance with the reporting requirements herein. For Unsuccessful Security Incidents, Business Associate shall provide Covered Entity, upon its written request, a report that: (a) identifies the categories of Unsuccessful Security Incidents; (b) indicates whether Business Associate believes its current defensive security measures are adequate to address all Unsuccessful Security Incidents, given the scope and nature of such attempts; and (c) if the security measures are not adequate, the measures Business Associate will implement to address the security inadequacies.

2.16. *Cooperation with Violations*. Business Associate will cooperate with Covered Entity's investigation and/or risk assessment with respect to any report made pursuant to Section 2.14, will abide by Covered Entity's decision with respect to whether such acquisition, access, Use or Disclosure constitutes a Breach of PHI and will follow Covered Entity's instructions with respect to any event reported to Covered Entity by Business Associate pursuant to Section 2.14. Business Associate shall maintain complete records regarding any event requiring reporting for the period required by 45 C.F.R. 164.530(j) or such longer period as may be required by state law and shall make such records available to Covered Entity promptly upon request but in no event later than within five (5) business days.

2.17. *Mitigation*. Business Associate agrees to mitigate, at its sole expense: (i) any harmful effect resulting from a Security Incident involving PHI or any Use or Disclosure of PHI by Business Associate or its Subcontractors in violation of the requirements of this Agreement, the HIPAA Regulations, or other applicable law; and (ii) any risks identified or discovered as a result of an Unsuccessful Security Incident.

2.18. *Breach*. In the event of a Breach of PHI arising out of the acts or omissions of Business Associate or any permitted agent or permitted Subcontractor of Business Associate and as instructed by Covered Entity, Business Associate agrees to either perform at its sole cost and expense, or pay the cost of Covered Entity's performance of, reasonable mitigation or

remediation services which shall include at a minimum: (i) reimburse Covered Entity for the cost of providing any notice to individuals affected by the Breach as Covered Entity reasonably determines to be required; (ii) at its own expense, providing any required notice of the Breach to government agencies, media, and/or other entities as Covered Entity reasonably determines to be required; (iii) if required by applicable law, providing individuals affected by the Breach of Protected Health Information with credit protection services designed to prevent fraud associated with identity theft crimes for a specific period not to exceed twelve (12) months, except to the extent applicable law specifies a longer period for such credit protection services, in which case such longer period shall then apply; (iv) providing reasonable contact support in the form of a toll-free number for affected individuals for a specific period not less than ninety (90) calendar days, except to the extent applicable law specifies a longer period of time for such contact support, in which case such longer period shall then apply; vi) paying reasonable fees associated with computer forensics work required for investigation activities related or relevant to the Breach of Protected Health Information; (vii) paying nonappealable fines or penalties assessed by governments or regulators; (viii) paying reasonable costs or fees associated with any obligations imposed by applicable law, including HIPAA, in addition to the costs and fees defined herein; and (ix) undertaking any other action both Parties agree to be appropriate.

2.19. *No Remuneration for PHI.* Business Associate shall not receive remuneration, either directly or indirectly, in exchange for PHI, except as may be permitted by Section 13405(d) of the HITECH Act or any regulations adopted as a result of that provision.

2.20. *Activities Outside the United States*. Business Associate represents that neither it nor any permitted agents nor permitted Subcontractors will transfer, access or otherwise handle Protected Health Information outside the United States without the prior written consent of Covered Entity.

3. **Responsibilities of Covered Entity.** With regard to the use and/or disclosure of PHI by Business Associate, Covered Entity hereby agrees to do the following:

3.1. Covered Entity may only upload, add or provide PHI to Business Associate's cloud services that is: (i) captured through Covered Entity's use of body worn cameras purchased from Business Associate ("BWC") or (ii) information strictly necessary to identify or categorize the PHI captured by BWC and uploaded to Business Associate's cloud services, but excluding, without limitation, any information describing or documenting an Individual's diagnosis, treatment, or Genetic information that is not captured by BWC.

3.2. Covered Entity shall manage its own data.

3.3. Covered Entity will make its privacy practices available at https://nebraskamed.com/patients/rights-responsibilities/notice-privacy-practices for Business Associate's review.

3.4. Inform Business Associate of any changes in, or revocation of, the permission by an individual to use or disclose PHI, to the extent such limitation may affect Business Associate's use or disclosure of PHI.

3.5. Notify Business Associate, in writing and in a timely manner, of any restriction on the use or disclosure of PHI that Covered Entity has agreed to or is required to abide by

under 45 C.F.R. § 164.522, to the extent that such restriction may impact in any manner the use and/or disclosure of PHI by Business Associate under this Agreement.

3.6. Not request Business Associate to use or disclose PHI in any manner that would not be permissible under the Privacy and Security Rules if done by Covered Entity.

3.7. Promptly notify Business Associate of any breach by Covered Entity of the Privacy or Security Rules.

4. **Standard Transactions**. To the extent Business Associate conducts on behalf of Covered Entity all or part of a Transaction, Business Associate shall comply with the Electronic Transactions Rule.

5. **Term and Termination**.

5.1. *Term.* This Agreement begins on the Effective Date and remains in effect until the Business Associate ceases to perform the Services for Covered Entity.

5.2. *Termination.* Either party may terminate this Agreement in the event it determines that the other party has violated a material term of this Agreement and such violation has not been remedied within ten (10) days following written notice to the violating party.

5.3. *Survival.* Except as otherwise expressly provided in this Agreement, all covenants, agreements, representations and warranties, express and implied, shall survive the execution of this Agreement, and shall remain in effect and binding upon the Parties until they have fulfilled all of their obligations hereunder, and the statute of limitations shall not commence to run until the time such obligations have been fulfilled. Any terms of this Agreement that must survive the expiration or termination of this Agreement in order to have their intended effect shall survive the expiration or termination of this Agreement whether or not expressly stated.

5.4. *Duties Upon Termination.* Upon termination of this Agreement, Business Associate shall allow Covered Entity to retrieve all PHI in the possession or control of Business Associate or its agents and Subcontractors and shall then destroy all PHI in its possession or control, as further set forth in the Underlying Agreement. However, if Business Associate determines that neither return nor destruction of PHI is feasible, Business Associate may retain PHI, provided that it extends the protections of this Agreement to the information and limits further Uses and Disclosures to those purposes that make the return or destruction of the information infeasible.

6. **General Provisions**

6.1. *Affiliated Covered Entity (ACE).* Covered Entity represents and warrants that it is an affiliate of the other Covered Entities listed on Exhibit A, and together Covered Entity and the Covered Entities listed in Exhibit A are members of an "Affiliated Covered Entity" as defined in 45 C.F.R. § 164.105. As such, the parties agree that it is their intention that this Agreement applies to Covered Entity and all Covered Entities listed on Exhibit A pursuant to the signature of Company.

6.2. *No Third Party Beneficiaries*. This Agreement is for the sole benefit of the Parties, and there are no third-party beneficiaries to the Agreement.

6.3. *Future Amendments to HIPAA or HIPAA Regulations*. To the extent HIPAA and/or the HIPAA Regulations are amended in the future and to the extent such amendments contain requirements and/or provisions not already contained in this Agreement required to be incorporated into this Agreement, the Parties agree that either (i) this Agreement shall be deemed to be automatically amended to the extent necessary to incorporate such additional requirements and/or provisions, or (ii) if determined necessary by Covered Entity, they will attempt in good faith to negotiate an amendment to this Agreement in order to incorporate any such additional requirements and/or provisions, provided that in the event that the Parties are unable to agree to such an amendment within sixty (60) days, either Party may terminate this Agreement upon thirty (30) days written notice to the other Party.

6.4. *Indemnification*. Business Associate agrees to indemnify and hold harmless Covered Entity from any and all liability, damages, costs (including reasonable attorneys' fees and costs) and expenses imposed upon or asserted against Covered Entity arising out of any claims, demands, awards, settlements or judgments relating to any breach of the terms of this Agreement by Business Associate, including, but not limited to, any Use or Disclosure of PHI by Business Associate, or its agents or Subcontractors that is contrary to the provisions of this Agreement or applicable law. This Section shall survive the termination or expiration of this Agreement.

6.5. *Limitation of Liability*. EXCEPT TO THE EXTENT SUCH LIMITATIONS ARE PROHIBITED BY APPLICABLE LAW, BUSINESS ASSOCIATES CUMULATIVE LIABILITY TO ANY PARTY FOR ANY LOSS OR DAMAGE RESULTING FROM ANY CLAIM, DEMAND, OR ACTION ARISING OUT OF OR RELATING TO THIS AGREEMENT WILL NOT EXCEED ONE (1) MILLION USD. NEITHER PARTY WILL BE LIABLE FOR DIRECT, SPECIAL, INDIRECT, INCIDENTAL, PUNITIVE OR CONSEQUENTIAL DAMAGES, HOWEVER CAUSED, WHETHER FOR BREACH OF WARRANTY OR CONTRACT, NEGLIGENCE, STRICT LIABILITY, TORT OR ANY OTHER LEGAL THEORY.

6.6. *Insurance*. Business Associate agrees to keep in full force and effect and maintain at its sole cost and expense a policy of data breach and cyber liability insurance covering theft, loss, or unauthorized Disclosure of Protected Health Information, personally identifiable nonpublic information or third-party corporate information in the care, custody or control of Business Associate in an amount sufficient to cover Business Associate's obligations hereunder, regardless of when the claim is brought, which amount shall be not less than ten million dollars ($10,000,000) per occurrence, ten million dollars ($10,000,000) aggregate. All insurance shall name Covered Entity as a certificate holder, and Business Associate shall furnish or cause its insurance carrier to furnish a certificate of insurance to Covered Entity as evidence of such agreement on the Effective Date hereof. This insurance shall be not changed or canceled without Business Associate providing at least thirty (30) days' prior written notice to Covered Entity (unless such cancellation is due to nonpayment of premiums, in which event ten (10) days' prior written notice shall be provided).

6.7. *No Assignment*. Business Associate's duties under this Agreement may not be transferred, assigned or assumed by any other person, in whole or in part, without the prior written consent of Covered Entity. Subject to the foregoing, this Agreement shall be binding upon, and shall inure to the benefit of, the Parties hereto and their respective permitted successors and assigns.

6.8. *No Ownership*. Any Protected Health Information provided by Covered Entity, its employees, agents, consultants or Subcontractors to Business Associate, or created, obtained, procured, Used or accessed by Business Associate on Covered Entity's behalf, shall at all times be and remain the sole property of Covered Entity, and Business Associate shall not have or obtain any rights therein except as stated herein.

6.9. *Remedies*. The Parties agree that the remedies at law for a violation of the terms of the Agreement may be inadequate and that monetary damages resulting from such violation may not be readily measured. Accordingly, in the event of a violation by either Party of the terms of the Agreement, the other Party shall be entitled to immediate injunctive relief. Nothing herein shall prohibit either Party from pursuing any other remedies that may be available to either of them for such violation.

6.10. *Independent Contractors*. It is expressly agreed that Business Associate, including its employees and Subcontractors, are performing services for Covered Entity as independent contractors. Neither Business Associate nor any of its employees, agents or Subcontractors is an employee or agent of Covered Entity. Nothing in this Agreement shall be construed to create (i) a partnership, joint venture or other joint business relationship between the Parties or their affiliates, or (ii) an agency relationship for purposes of the HITECH Act.

6.11. *Notices*. All notices and other communications required under this Agreement will be in writing, addressed to either party to the attention of its Privacy Officer at its address set forth above, and will be deemed effectively delivered (i) upon personal delivery, or (ii) upon receipt from a courier service as confirmed by written verification of receipt. Either party may change its address for such communications by giving an appropriate notice to the other party in conformity with this Section.

If to Covered Entity:
University of Nebraska Medical Center
988102 Nebraska Medical Center
Omaha, NE 68198-8102
Attn: Privacy Officer

With a copy to:
University of Nebraska
6001 Dodge Street
Omaha, NE 68182
Attn: Chief Compliance Officer

If to Business Associate:
Axon Enterprise, Inc.
17800 N 85th Street
Scottsdale, AZ 85255
Attn: General Counsel

6.12. *Counterparts*. This Agreement may be executed in counterparts, each of which shall be deemed an original but all of which shall constitute one and the same instrument. An executed Agreement delivered by facsimile or other electronic transmission shall be treated as if an original.

[Signatures on the following page]

IN WITNESS WHEREOF, the parties hereto have caused their authorized representatives to execute this Agreement as of the dates set forth below.

The Board of Regents of the University of Nebraska

By: Chris Kabourek

Name: Chris Kabourek

Title: Senior VP | CFO

Date: 12/21/22 | 12:48 CST

Axon Enterprise, Inc.

By: DocuSigned by: Robert E Driscoll 55DAEBB131A4424...

Name: Robert E Driscoll

Title: VP, Assoc. General Counsel

Date: 12/16/2022 | 12:06 PM MST

EXHIBIT A

ACE Covered Entities

The Nebraska Medical Center, located at 987400 Nebraska Medical Center, Omaha, NE 68198-7400

Bellevue Medical Center, located at 2500 Bellevue Medical Center Drive, Bellevue, NE 68123