

Agreement No. _____

**COUNTY OF KINGS
AGREEMENT FOR TECHNOLOGY SERVICES**

This Agreement for Technology Services (“Agreement”) is made and entered into on _____, 2026 (“Effective Date”), by and between the County of Kings, a political subdivision of the State of California (“County”), and **Axon Enterprise, Inc.** (“Contractor”) (singularly a “Party,” collectively the “Parties”).

R E C I T A L S

WHEREAS, the County requires digital evidence management services;

WHEREAS, Contractor has submitted a quote for such services, which the County has accepted; and

WHEREAS, Contractor is ready, willing, able, and qualified to perform such services.

NOW, THEREFORE, the Parties agree as follows:

1. SCOPE OF SERVICES

Contractor shall provide the services as described herein (collectively, the “Services”), which may be described in more detail in a Digital Evidence Management Solution document and Quote specifying the terms and conditions for such Services, in substantially the form attached hereto as **Exhibits A and B** (each an individual “SOW”).

2. RESPONSIBILITIES OF CONTRACTOR

Contractor possesses the requisite skills necessary to perform the work under this Agreement and the County relies upon such skills. Contractor shall, at all times, utilize its ability, experience, and talent to faithfully, industriously, and professionally perform the work set forth in the SOW to the County’s reasonable satisfaction. The Services to be performed by Contractor will be performed in a timely, professional, and workman-like manner, in accordance with industry standards, and with a degree of care, skill, and expertise, as is required for the provision of services of a similar nature. The County’s acceptance of Contractor’s work does not constitute a release of Contractor from its professional responsibility.

Contractor affirms that it possesses all necessary federal, state, and local permitting, licensure, and certification required to perform the work under this Agreement, including,

but not limited to, valid driver's license(s), professional license(s), or certificate(s) of tax-exempt status.

3. COMPENSATION

Subject to the terms and conditions of this Agreement, the County will pay Contractor the fees specified in Axon Quote Q-810611-46108MK, attached hereto and fully incorporated herein as **Exhibit B** (collectively, the "Fees"). Contractor agrees that such Fees constitute the full and complete consideration for Contractor's performance of Services hereunder, for all rights acquired by the County, and that no other fees will be owed by the County under this Agreement.

County shall pay Contractor annually, up to the maximum amount reflected in the SOW, within thirty (30) days of receipt of timely invoices. Contractor shall submit invoices to County describing the Services rendered, to whom, the date(s) of service, and the charges in a form approved by the County. Invoices must be documented in such reasonable detail as required by the County's Auditor to determine whether the funds were expended for the intended purposes. Contractor shall support its costs by properly executing payrolls, time records, attendance records, billing statements, contracts, detailed ledgers, vouchers, orders, or any other documents pertaining in whole or in part to this Agreement.

Should no funds or insufficient funds be appropriated for this Agreement, the County reserves the right to propose an amendment or unilaterally terminate this Agreement immediately.

4. TERM

The term of the Agreement will commence on the **Effective Date** and will continue thereafter for the initial term specified in the SOW. This Agreement may be extended upon the mutual written consent of the Parties, as evidenced by a duly executed renewal or extension document signed by authorized representatives of both Parties.

5. RECORDS AND INSPECTIONS

Contractor shall maintain full, complete, and accurate records with respect to all matters covered under this Agreement. Contractor shall: (a) prepare all records in accordance with generally accepted accounting procedures; (b) clearly identify the records; (c) keep said records readily accessible; and (d) maintain the records for seven (7) years after the termination of this Agreement. County shall have reasonable access during normal work hours to such records and the right to examine, inspect, copy, or audit them, at no cost to County.

///

6. AMENDMENTS

The Parties may modify this Agreement only by a written amendment signed by the Contractor and the County's Board of Supervisors ("Board") or other representative as authorized by the Board.

7. TERMINATION

The right to terminate this Agreement may be exercised without prejudice to any other right or remedy to which the terminating Party may be entitled at law or under this Agreement.

A. Non-Appropriation. If the County's funding for the Services under this Agreement becomes unavailable, the County may terminate this Agreement effective immediately.

B. With Cause. This Agreement may be terminated by either Party should the other Party materially breach its duties or responsibilities hereunder. Upon determining whether a material breach has occurred, the non-breaching Party shall provide written notice to the breaching Party of its intention to terminate this Agreement and inform the breaching Party whether the breach is able to be cured or not.

1) Breach Subject to Cure. Unless otherwise specifically noted in the Notice of Breach, all Notices of Breach shall be deemed subject to this provision. If the non-breaching Party deems the breach of a nature subject to cure, said Party shall allow the breaching Party a period of at least thirty (30) calendar days to cure the breach. If the breach is not remedied within the period specified in the Notice of Breach, the non-breaching Party may terminate the Agreement upon further written notice specifying the date of termination.

a. In the event the nature of the breach requires more time than allowed in the Notice of Breach to cure, the breaching Party may submit a written proposal to the non-breaching Party within that period, setting forth a specific plan to remedy the breach and the date certain for completion. If the non-breaching Party assents to the proposed plan in writing, the breaching Party shall immediately commence curing the breach. If the breaching Party fails to cure the breach within said period, the non-breaching Party may terminate this Agreement: (a) immediately; (b) on the date specified in the Notice of Breach; or (c) grant the breaching Party additional time to cure.

b. If Contractor is the breaching Party, the County may elect to cure the breach, and Contractor shall bear all reasonable expenses incurred by the County in curing the breach.

2) Breach Not Subject to Cure. If the non-breaching Party deems the breach is of such a nature as it is not subject to or is incapable of being cured, that Party shall provide a Notice of Breach to the breaching Party of its intent to terminate this Agreement, in which it shall include a date upon which the Agreement terminates.

C. Effects of Termination. Upon termination of this Agreement or any SOW, Contractor shall immediately refund to the County all amounts pre-paid by the County for Services that were to be provided after such termination. Termination of this Agreement shall not terminate Contractor's obligations or liability to the County for damages sustained by the County because of the Contractor's breach, nor the Contractor's duty to indemnify, maintain, and make available any records pertaining to this Agreement, cooperate with any audit, or make any reports of pre-termination contract activities. Upon the delivery by a Party of its notification of termination of this Agreement or any SOW, the Parties shall reasonably cooperate with each other to transition the Services and all work in progress to the County or its designee, and such reasonable cooperation shall include, Contractor's obligation to reasonably mitigate any costs and expenses associated with such transition and Contractor's obligation to transition any data, know-how, or other similar materials to the County or its designee.

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

D. No Waiver of Breach or Breach by Forbearance. In no event will either Party's act of forbearance regarding previous acts by the other Party: (a) constitute a breach under this Agreement; (b) waive a Party's right to assert breach or breach; nor (c) impair or prejudice any remedy available to the non-breaching Party.

8. INSURANCE

A. Requirement to Obtain, Maintain, and Deliver Proof of Insurance. Without limiting the County's right of indemnification from Contractor or any third parties, Contractor shall purchase and maintain the insurance policies described below (the "Insurance Policy(ies)"), prior to the commencement of work or execution of this

Agreement. Contractor shall maintain the Insurance Policy(ies) throughout the term of this Agreement.

B. Endorsed Additional Insured. Contractor shall deliver an Endorsed Additional Insured page from Contractor's insurance carrier to the County guaranteeing said coverage to the County, prior to execution of this Agreement or commencing work. Contractor shall deliver proof of insurance and all endorsements in accordance with this Agreement's Notice Section. Failure to obtain, maintain, or provide the Insurance Policy(ies) or proof of the same is a material breach of this Agreement and may result in the immediate suspension or termination of this Agreement for cause, in addition to any other remedies the County may have under the law.

C. Endorsement of Policies. Contractor shall cause each of the Insurance Policy(ies) to be endorsed designating the County and its Board members, officials, officers, employees, and agents as additional insureds, using ISO form CG 20 26 or an alternate form that is at least as broad as form CG 20 26, as to any liability arising from the performance of this Agreement.

D. Insurance Limits. Contractor shall obtain the Insurance Policy(ies) in the amounts set forth below:

1. Commercial General Liability covering bodily injury, personal injury, and property damage with minimum limits of Two Million Dollars (\$2,000,000) per occurrence and Four Million Dollars (\$4,000,000) annual aggregate.

2. Comprehensive Automobile Liability covering (a) bodily injury of not less than Five Hundred Thousand Dollars (\$500,000) per person and One Million Dollars (\$1,000,000) per accident, and property damage of not less than One Hundred Thousand Dollars (\$100,000); or (b) coverage with a combined single limit of One Million Dollars (\$1,000,000). The Comprehensive Automobile Liability must cover owned and non-owned vehicles used in connection with this Agreement.

3. Workers' Compensation as required by the California Labor Code. Contractor shall cause said Insurance Policy(ies) to be endorsed to waive the insurer's subrogation rights against the County.

4. Technology Professional Liability Errors and Omissions Insurance appropriate to Contractor's profession and work hereunder, with limits not less than Two Million Dollars (\$2,000,000) per occurrence. Coverage shall be sufficiently broad to respond to the duties and obligations as is undertaken by Contractor in this Agreement and shall include, but not be limited to, claims involving security breach, system failure, data recovery, business interruption, cyber extortion, social engineering, infringement of intellectual property, including, but not limited to, infringement of copyright, trademark,

trade dress, invasion of privacy violations, information theft, damage to or destruction of electronic information, release of private information, and alteration of electronic information. The policy shall provide coverage for breach response costs, regulatory fines, and penalties, as well as credit monitoring expenses.

5. Umbrella or Excess Policies. Contractor may use Umbrella or Excess Policies to provide the liability limits as required in this Agreement. This form of insurance will be acceptable provided that all of the primary and Umbrella or Excess Policies shall provide all of the insurance coverages herein required, including, but not limited to, primary and non-contributory, additional insured, Self-Insured Retentions (SIRs), indemnity, and defense requirements. The Umbrella or Excess Policies shall be provided on a true “following form” or broader coverage basis, with coverage at least as broad as provided on the underlying Commercial General Liability insurance. No insurance policies maintained by the Additional Insureds, whether primary or excess, and which also apply to a loss covered hereunder, shall be called upon to contribute to a loss until the Contractor’s primary and excess liability policies are exhausted.

E. Rating of Insurers. Contractor shall obtain insurance placed with admitted insurers rated by A.M. Best Co. as A:VII or higher.

F. Notice of Cancellation to the County and Payment of Premiums. Contractor shall cause each of the Insurance Policy(ies) to be endorsed to provide the County with thirty (30) days’ prior written notice of cancellation. The County is not liable for the payment of premiums or assessments on any Insurance Policy(ies). Cancellation provisions in an Insurance Policy(ies) will not be construed in derogation of the continuing duty of the Contractor to maintain the Insurance Policy(ies) during the term of this Agreement.

9. CRIMINAL JUSTICE INFORMATION SERVICES COMPLIANCE

Contractor agrees to support County’s obligation to comply with the Federal Bureau of Investigation Criminal Justice Information Services (“CJIS”) Security Policy, incorporated herein, and shall comply with the terms of the CJIS Security Policy, available at <https://le.fbi.gov/cjis-division/cjis-security-policy-resource-center>, for Criminal Justice Information (“CJI”), to the extent applicable to the Services herein. Contractor shall protect CJI, Personal Information and/or other sensitive information in accordance with all relevant laws and regulations.

10. CLOUD SERVICES ADDENDUM AND SERVICE LEVEL AGREEMENT

A. Cloud Services Addendum. To the extent Contractor delivers any cloud-based services under this Agreement, such services shall be governed by the terms and conditions set forth in the Cloud Services Addendum, attached hereto as **Exhibit C** (the

“Cloud Services Addendum” or “CSA”), and the Axon Appendices, attached hereto as **Exhibit E**. The Cloud Services Addendum includes, among other things, provisions related to data retention and disposal, data transfer upon termination or expiration, support obligations, and data security requirements specific to cloud services. Contractor shall perform the Services in accordance with the standards and service levels set forth therein. In the event of any conflict between the terms of this Agreement and the Cloud Services Addendum with respect to the cloud services, the terms of the Cloud Services Addendum shall control.

B. Service Level Agreement. Contractor shall perform the Services in accordance with the service levels set forth in the Service Level Agreement, attached hereto as **Exhibit D** (the “Service Level Agreement”). Contractor will use commercially reasonable efforts to meet or exceed the service levels described therein. County will be entitled to the remedies specified in the Service Level Agreement in the event of any failure by Contractor to meet the applicable service levels.

11. INDEMNIFICATION

A. Professional Services. When the law establishes a professional standard of care for Contractor’s services, to the fullest extent permitted by law, Contractor shall indemnify, defend, and hold harmless County, and any and all of its Board members, officials, employees, and agents, from and against any and all third-party losses, liabilities, damages, costs, and expenses, including legal counsel’s reasonable fees and costs, but only to the extent Contractor such damages, liabilities, and costs are caused by Contractor’s negligent act or willful omission. Contractor shall not be obligated to defend or indemnify the County for its own negligence or for the negligence of third parties.

B. All Other Services. Other than in the performance of professional services, including agreements where professional services will be provided along with other types of services, and to the fullest extent permitted by law, Contractor shall indemnify, defend, and hold harmless the County, and any and all of its Board members, officials, employees, and agents, from and against any third-party claims for liability (including liability for claims, suits, actions, arbitration proceedings, administrative proceedings, regulatory proceedings, losses, expenses, or costs of any kind, whether actual, alleged, or threatened, including reasonable attorneys’ fees and costs, court costs, interest, defense costs, and expert witness fees), where the same arise out of, are a consequence of, or are in any way attributable to, in whole or in part, relating to: (a) the failure by Contractor to comply with all applicable laws and regulations in the performance of its obligations under this Agreement; (b) any claim the Services infringe or misappropriate a third party’s intellectual property rights, including patents, copyrights, trademarks, or trade secrets; or (d) any intentional misconduct or gross negligence by Contractor, including, but not limited to, officers, employees, or subcontractors of Contractor in performing the Services.

C. Indemnification Procedure. In the event of any third-party claim, demand, suit, investigation, or action (a "Claim") for which the County is or may be entitled to indemnification hereunder, Contractor agrees to be solely responsible for defending the Claim, subject to the County's right to participate with counsel of its own choosing, at its own expense, and for payment of all judgments, settlements, damages, losses, liabilities, costs, and expenses, including reasonable attorneys' fees, resulting from the Claim against the County, provided that the Contractor will not agree to any settlement that imposes any obligation, liability, or admission of fault on the County without the County's prior written consent, which shall not unreasonably be withheld.

D. Intentionally Omitted.

E. These indemnification obligations shall survive the termination of this Agreement as to any negligent act, willful omission, fault, or negligence occurring during this Agreement or any extension of this Agreement. The County's rights to indemnification are in addition to and shall not limit any other rights or remedies the County may have under law or this Agreement.

12. LIMITATION OF LIABILITY

In no event will either Party be liable for any consequential, indirect, exemplary, punitive, special, or incidental damage(s) arising from or relating to this Agreement, whether or not they have been advised of the possibility of such damage(s), and regardless of the nature of the cause of action asserted. Contractor's 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 the purchase price paid to Contractor for the Contractor Device, or if for Services, the amount paid for such Services over the twelve (12) months preceding the claim.

13. INDEPENDENT CONTRACTOR

Contractor is an independent contractor and not an agent, officer, or employee of the County. This Agreement is by and between two (2) independent contractors and is not intended to, nor will it be construed to create the relationship of agent, servant, employee, partnership, joint venture, or association.

14. COMPLIANCE WITH LAW

Contractor shall comply with all federal, state, and local laws and regulations applicable to its performance, including, but not limited to, Government Code section 8350, et seq. regarding a drug free workplace, all health and safety standards set forth by the State of California and County, and the California Public Records Act, Government Code section 7920.000, et seq.

15. CONFLICT OF INTEREST

Contractor warrants that its board of directors, employees, officers, including the immediate families of each, have no financial interest, direct or indirect, that conflicts with rendering the Services under this Agreement and will not acquire any such financial interest. Contractor shall not employ nor retain any such person during the term of this Agreement. Contractor is not relieved from personal responsibility under this Section 14 by their associates and employees rendering the Services. Contractor has an affirmative duty to and shall disclose the name(s) of any person(s) who have an actual, potential, or apparent conflict of interest.

16. NONDISCRIMINATION

In rendering the Services under this Agreement, Contractor shall comply with all applicable federal, state, and local laws, rules, and regulations and shall not discriminate based on age, ancestry, color, gender, marital status, medical condition, national origin, physical or mental disability, race, religion, gender identity, gender expression, sexual orientation, military status, or any other protected basis.

Further, Contractor shall not discriminate against its employees, which includes, but is not limited to, employment upgrading, demotion or transfer, recruitment or recruitment advertising, layoff or termination, rates of pay or other forms of compensation, and selection for training, including apprenticeship.

17. SUBCONTRACTORS

Services under this Agreement are personal services. Contractor shall not subcontract any work under this Agreement without the prior written consent of the County, subject to any required state or federal approval.

18. ASSIGNMENT

Neither Party may assign this Agreement without the other Party's prior written consent. Contractor 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. Assignment by Contractor of any monies due does not constitute an assignment of this Agreement.

19. UNFORESEEN CIRCUMSTANCES

Neither Party shall be responsible for any act of God; fire, flood; storm; inclement weather; earthquake; drought; riot; war or insurrection; epidemic; pandemic; plant or

animal infestation or disease; sudden or severe energy shortage, civil disturbance, labor dispute, or other cause beyond the reasonable control of a Party, on the condition the affected Party notices the other Party in writing of the delay's cause within ten (10) of the date the delay began, or as soon thereafter as reasonably practicable in the event that notification during this time frame is not possible due to the respective condition. Thereafter, the Parties shall meet and confer as to whether to amend, suspend, or terminate this Agreement.

20. OWNERSHIP OF DOCUMENTS

The County owns and is entitled to possess all computations, plans, correspondence, pertinent data, and information gathered by or computed by Contractor solely and exclusively in connection with this Agreement, prior to this reuse of any such materials in a manner other than originally intended is at the County's sole risk. Material prepared solely and exclusively in connection with this Agreement is not subject to copyright in the United States of America or in any foreign state.

21. NOTICE

The Parties shall give any notice necessary to the performance of this Agreement in writing, and deliver by personal delivery, fax, overnight carrier, e-mail with read receipt acknowledgment, or by prepaid first-class mail, addressed as follows:

County

Morgan Elias, Fiscal Analyst
Kings County District Attorney
1400 West Lacey Boulevard
Hanford, CA 93230

Contractor

Attn: Legal
Axon Enterprise, Inc.
17800 N. 85th Street
Scottsdale, AZ 85255
Email: legal@axon.com

Notice given by: (a) personal delivery is effective on the date of personal delivery; (b) fax is effective on date of transmittal; (c) overnight carrier is effective on the date of delivery; (d) e-mail is effective on the date of delivery, with a read receipt; or (e) prepaid first-class mail is effective five (5) days after the date of mailing, or the delivery date on the return receipt, whichever occurs first.

22. CHOICE OF LAW

The Parties executed and delivered this Agreement in the County of Kings, State of California. The laws of the State of California govern the validity, enforceability, and interpretation of this Agreement. Kings County is the appropriate venue for bringing any action in connection with this Agreement, whether in law or equity. Contractor waives any rights it may possess under California Code of Civil Procedure section 394 to transfer any

action arising out of this Agreement to a neutral county or alternate venue. The Parties expressly agree that either Party may appear for and attend all matters, remotely via teleconference or videoconference at the party's discretion, to the extent allowable by court.

23. SEVERABILITY

If a court of competent jurisdiction finds any of the provisions of this Agreement unenforceable, the remaining provisions remain enforceable and the unenforceable provisions constitute an amendment to the limited extent required to permit enforcement of the Agreement as a whole.

24. LEGAL FEES

The prevailing Party in any litigation between the Parties relating to this Agreement will be entitled to recover its reasonable attorneys' fees and court costs, in addition to any other relief that it may be awarded.

25. SURVIVAL

Any and all obligations under this Agreement, which expressly state that they survive termination or expiration, as well as those provisions that by their nature should survive the termination or expiration of this Agreement, shall be deemed to survive the termination or expiration of this Agreement.

26. NO THIRD-PARTY BENEFICIARIES

Unless otherwise specifically stated in this Agreement, the County and Contractor are the only Parties to this Agreement and the only Parties entitled to enforce its terms. Nothing in this Agreement gives, is intended to give, or will be construed to grant any right or benefit to a third party, directly, indirectly, or otherwise.

27. ENTIRE AGREEMENT; CONTRIBUTIONS OF BOTH PARTIES

This Agreement, including its Recitals and Exhibits, are fully incorporated into and are integral parts of this Agreement. This Agreement constitutes the entire agreement between the Parties. There are no inducements, promises, terms, conditions, or obligations made or entered into by the County or Contractor, other than those contained herein this Agreement.

Each Party had an opportunity to review this Agreement, consult with legal counsel, and negotiate terms. Contractor waives the rule under Civil Code section 1654, that ambiguities in a contract should be construed against the drafter. Civil Code section 1654

has no application to the construction of the Agreement. In the event of any conflict between this Agreement and a SOW, this Agreement will control unless the SOW expressly refers to the Parties' intent to alter the terms of this Agreement with respect to that SOW.

28. ELECTRONIC SIGNATURES; COUNTERPARTS

The Parties may execute this Agreement by electronic means, and in two (2) or more counterparts that together constitute one (1) Agreement. Digital signatures must meet the requirements under Government Code section 16.5 to be valid.

29. AUTHORITY

Each signatory to this Agreement represents it is authorized to enter into this Agreement and bind the Party that its signature represents.

REMAINDER OF PAGE INTENTIONALLY BLANK

SIGNATURES ARE ON FOLLOWING PAGE

IN WITNESS WHEREOF, the Parties executed this Agreement on the Effective Date first written above.

COUNTY OF KINGS

AXON ENTERPRISE, INC.

By: _____
Rusty Robinson, Board Chairman
Kings County Board of Supervisors

Signed by:
Robert Driscoll 5/26/2026 | 12:44 PM MST
55DAEBB131A4424...
By: _____
Robert Driscoll, Deputy General Counsel

ATTEST

By: _____
Catherine Venturerlla, Clerk of the Board

RISK MANAGEMENT APPROVED AS TO INSURANCE

By: B. Yepez for _____
Sarah Poets, Risk Manager

APPROVED AS TO FORM
Laurie Avedisian-Favini, County Counsel

By: Jennifer Thompson
Jennifer Thompson, Deputy County Counsel

Exhibits/Attachments:

- Exhibit A:** Digital Evidence Management Solution
- Exhibit B:** Axon Quote Q-810611-46108MK
- Exhibit C:** Cloud Services Addendum
- Exhibit D:** Service Level Agreement
- Exhibit E:** Axon Appendices

{4916-9317-8782, v.2}

Exhibit A

Digital Evidence Management Solution

AXON JUSTICE PREMIER+

DIGITAL EVIDENCE MANAGEMENT SOLUTION

Prepared By: Molly Kinsella

Email: mkinsella@axon.com

Phone: 480-805-5496

17800 North 85th Street

Scottsdale, AZ 85255

2-28-2025



EXECUTIVE SUMMARY 3

THE DIGITAL EVIDENCE WORKFLOW 5

AXON JUSTICE OVERVIEW 6

 EVIDENCE INTAKE METHODS 7

 UNLIMITED EVIDENCE STORAGE AND SECURITY 9

 EVIDENCE PROCESSING AND REVIEW 11

 VIDEO PLAYBACK, EDITING, AND EXHIBIT CREATION 16

 CASE ROUTING, NOTIFICATIONS, AND ACCESS CONTROL 18

 DISCOVERY AND EXTERNAL SHARING 21

 THIRD-PARTY SYSTEM INTEGRATIONS 22

 AXON JUSTICE HARDWARE ADD-ONS 24

AXON JUSTICE DEPLOYMENT PROCESS 25

OUR EXPERIENCE 28

APPENDIX 29

 APPENDIX A 30

TABLE OF CONTENTS



EXECUTIVE SUMMARY



Digital evidence is now central to every criminal case, yet many legal teams struggle to efficiently manage, review, and disclose case-critical data at scale. Legal teams must process video footage, audio recordings, forensic reports, and digital communications while meeting strict discovery requirements and courtroom deadlines. The growing complexity of digital evidence demands a structured, scalable system that helps

limit inefficiencies while maintaining the integrity of case materials from collection to resolution.

For over three decades, Axon has provided law enforcement, prosecutors, and defense attorneys with tools that support case preparation, evidence organization, discovery and operational efficiency. As digital evidence continues to expand across law enforcement, public safety, and private sector sources, agencies relying on disconnected storage, manual file transfers, and fragmented workflows face growing challenges in tracking critical evidence, maintaining chain of custody, and preparing cases efficiently.

Axon Justice is designed to bridge these gaps—offering a centralized, scalable Digital Evidence Management System (DEMS) that connects legal teams to a vast and structured digital evidence ecosystem, streamlining ingestion, review, and disclosure while supporting seamless collaboration across justice stakeholders.

A DIRECT CONNECTION TO ONE OF THE LARGEST DIGITAL EVIDENCE ECOSYSTEMS

With more than 21,000 agencies and organizations using Axon solutions, Axon Justice provides unmatched access to one of the most expansive digital evidence ecosystems in the world. This unparalleled network allows organizations to seamlessly share between each other at scale.

Unlike standalone evidence systems, Axon Justice ingests and organizes evidence from:

- ▶ LAW ENFORCEMENT AGENCIES using body-worn cameras, in-car video, all collected case evidence and investigative tools
- ▶ ENTERPRISE SECURITY TEAMS in retail, corporate, and private sectors
- ▶ PUBLIC SAFETY AGENCIES including fire, EMS, and campus security
- ▶ THIRD-PARTY SOURCES such as forensic labs, citizen-submitted videos, and surveillance footage

This broad network of evidence—spanning public, private, and corporate sectors—feeds directly into Axon Justice, where legal teams can search, review, and disclose case materials with confidence.

By connecting justice agencies to a vast and structured evidence network, Axon Justice simplifies the case intake process and improves case readiness, transparency, and overall efficiency.



BENEFITS OF AXON JUSTICE

- ▶ **CENTRALIZED DIGITAL EVIDENCE MANAGEMENT** – Consolidates evidence from body-worn cameras, cloud storage, and physical media into a single, secure system, reducing inefficiencies and protecting evidence integrity.
- ▶ **FASTER EVIDENCE REVIEW WITH AI AND AUTOMATION** – AI-powered transcription, translation, and summarization tools accelerate the review of large volumes of video, audio, and digital files, allowing staff to focus on case strategy.
- ▶ **STREAMLINED DISCOVERY PROCESS** – Automates disclosures and tracking, helping legal teams organize, review, and share evidence without the stress of manual processing.
- ▶ **SEAMLESS SYSTEM INTEGRATION** – Axon Justice has a robust set of integration capabilities to integration with 3rd party systems like Case Management bringing critical systems together to improve efficiency.

HOW LEGAL TEAMS USE AXON JUSTICE

Axon Justice offers a user-friendly, structured solution that streamlines digital evidence management, replacing manual processes with more efficient workflows.

- ▶ **PROSECUTORS** – Can receive and organize digital evidence directly from law enforcement and other partners, without needing to manually track down files.
- ▶ **PUBLIC DEFENDERS** – Can access discovery materials through a secure portal instead of waiting for physical copies.
- ▶ **LEGAL TEAMS** – Can search, review, and prepare exhibits in one system, without needing multiple software programs.
- ▶ **COURTS AND FORENSIC ANALYSTS** – Can securely receive case materials to support trial preparation.

With everything stored, organized, and accessible in one place, Axon Justice makes managing digital evidence simpler, faster, and more secure.

“By putting Axon Justice Premier on every lawyer’s desk, we’re saving 88 full-time [video technician] positions across the state, and that’s a savings of almost \$3 million. And when you combine that with the transcription services we’re using Axon Justice for, we’re saving the taxpayers almost \$4 million just by having these tools on our desk.”

STEPHEN CRUMP // EXECUTIVE DIRECTOR
TENNESSEE DISTRICT ATTORNEY’S GENERAL
CONFERENCE



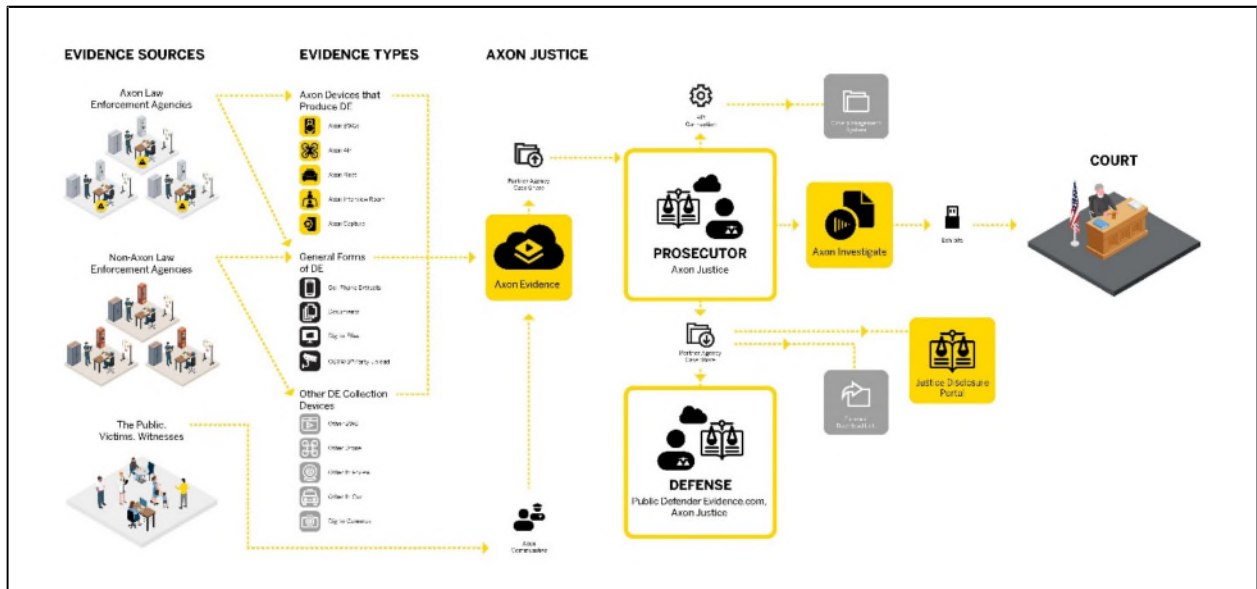
THE DIGITAL EVIDENCE WORKFLOW



Managing digital evidence requires a structured system that ensures accessibility, security, and seamless collaboration across legal teams. The Axon Justice workflow connects evidence sources, prosecutors, defense attorneys, and courts within a centralized Digital Evidence Management System (DEMS) to streamline case preparation and legal proceedings.

The process begins with evidence collected from various sources, including:

- ▶ LAW ENFORCEMENT AGENCIES USING AXON products to store their evidence.
- ▶ LAW ENFORCEMENT AGENCIES USING NON-AXON or on-premise solutions to store and organize their data, requiring the submission of case materials from third-party systems or physical media.
- ▶ PUBLIC SOURCES, VICTIMS, AND WITNESSES contributing digital evidence through various methods.



Legal Teams access and manage digital case materials in Axon Justice, where they can organize and analyze evidence, prepare exhibits and case files, and collaborate with investigative teams and external partners. Defense attorneys receive discovery materials through the Justice Disclosure Portal or their own Axon Justice platform, ensuring secure and structured access to case-related evidence.

This interconnected workflow ensures that digital case materials move seamlessly through the Axon Justice Digital Evidence Lifecycle—from initial collection and secure storage to review, discovery, and courtroom presentation. By streamlining each stage, Axon Justice improves efficiency, reduces administrative burdens, and strengthens the integrity of legal casework.



AXON JUSTICE OVERVIEW

Axon Justice provides legal teams with a centralized system to collect, organize, review, and share digital evidence efficiently. By streamlining workflows, automating key processes, and integrating with existing legal systems, Axon Justice ensures that case materials remain secure, accessible, and structured throughout the entire digital evidence lifecycle. The table below outlines how Axon Justice enhances digital evidence workflow at every step.

SECTION	DESCRIPTION
Evidence Intake	Focuses on the various technical and functional methods of getting various evidence types, from various sources into the Axon Justice system for routing and processing.
Unlimited Evidence Storage and Management	Provides UNLIMITED secure, structured storage of digital evidence in Axon Justice, ensuring scalability, compliance, and accessibility. Indexing, categorization, and advanced search tools enable legal teams to efficiently retrieve and organize case materials.
Evidence Processing and Review	Covers the numerous AI-Enabled review and authentication tools for analyzing and understanding the content of digital evidence that has been submitted to the office.
Video Playback, Editing, and Exhibit Creation	Provides tools to review, edit, and organize video evidence without the need for third-party software. Features include multi-angle playback, annotation tools, forensic video enhancement, and metadata tagging, enabling legal teams to quickly analyze, create, prepare, and present exhibits.
Case Routing, Notifications, and Access Control	Automates case assignment and evidence tracking through configurable routing workflows and notifications. Role-based access controls manage user permissions, while metadata fields (e.g., court numbers, case status) improve case organization and compliance tracking.
Discovery and External Sharing	Enables secure, trackable evidence sharing between prosecutors, defense attorneys, and courts. Disclosure portals, partner agency case shares, and structured external download links ensure an audit-tracked discovery process, maintaining strict access control and compliance.
Third-Party System Integrations	Connects Axon Justice to case management systems, forensic tools, and investigative applications via API-based integrations. Supports automated evidence transfers and secure, trackable data exchanges, reducing reliance on disconnected systems and manual processing.
Axon Justice Hardware Add-Ons	Expands digital evidence collection and management by integrating Axon body-worn cameras and interview room systems. Direct uploads to Axon Justice ensure high-quality video and audio evidence is securely captured, stored, and immediately accessible, reducing administrative burden and improving case-building workflows.



EVIDENCE INTAKE METHODS

Legal teams receive case materials from multiple sources through various methods and across scattered storage locations, creating inefficiencies and security risks.

- ▶ **NUMEROUS SOURCES** – Law Enforcement, victims, witnesses, citizens, expert witnesses, forensic analysts, and many more.
- ▶ **VARIOUS SUBMISSION METHODS** – Email, USBs, hard drives, cloud shares, and even paper.
- ▶ **STORAGE LOCATIONS** – Cloud and on-prem network drives, local desktops, DVDs, Hard Drives, and physical filing cabinets.

Current inefficient evidence intake and storage process create bottlenecks in case preparation and discovery management, forcing attorneys to search across network drives, CMS, desktops, and filing cabinets for scattered materials. Inconsistent submission formats add delays, while unstructured storage lacks audit trails, making it difficult to track access or modifications. Physical media like USBs and paper records are prone to loss or tampering, and email transfers increase security risks. Without a centralized digital evidence management system (DEMS) to automate tracking and secure case data, legal teams face compliance risks, administrative burdens, and evidentiary challenges.

Paramount to all the inefficiency, is the risk of data corruption. Every time data is copied, moved, downloaded or stored – users run the risk of losing meta data associated with the file. This not only has the potential to violate discovery obligations but also limits data for legal teams to make decisions with.

PARTNER	CURRENT INGESTION METHODS	CURRENT STORAGE SOLUTION
Law Enforcement Agency using Axon	Axon Partner Share	Axon Evidence DEMS / Network Drives / CMS / on-Prem servers
Law Enforcement Agency not using Axon	Physical Media, Cloud Shares from multiple providers, Email, Paper, 3 rd party DEMS	Network Storage, CMS, User Desktops, File Cabinets, Cellphone Forensics Storage
Digital Forensics Teams	Dedicated Server, Hard drives, media extraction tools	Dedicated Server, dedicated machine to run, Hard Drives duplicates for defense
Expert Witnesses, ME's Office, Business Partners	Physical Media, Cloud Shares, Email, Paper	Network Storage, CMS, User Desktops, File Cabinets, Cellphone Forensics Storage
Citizens, Victims, Witnesses	Physical Media, Cloud Shares, Email, Paper	Network Storage, CMS, User Desktops, File Cabinets, Cellphone Forensics Storage



UNIFYING EVIDENCE INTAKE

To fully leverage the unlimited storage and world-class security provided by Axon Justice, users need efficient tools to ingest a wide range of data from multiple sources at scale. With this purpose-built solution, you can seamlessly receive data from anywhere using one of the following methods that will allow organizations to have a single source of truth.

/ AXON NETWORK PARTNER SHARE

Axon's native cloud-to-cloud transfer system enables seamless data sharing between any users on the Axon Network. Agencies can easily set up sharing protocols with simple administrative approvals, while roles and permissions ensure that only authorized users can share data between organizations.

/ LEA INGEST PORTALS

Axon provides dedicated, agency-specific ingestion portals where officers can securely upload, organize, and share their data to prosecutors for discovery to defense. These sites are included at no additional cost to the law enforcement agency.

/ WEB BROWSER UPLOAD

Users can easily upload files using a standard browser-based interface. Users can drag and drop files directly into the platform, ensuring a quick and seamless experience.

/ EVIDENCE UPLOAD XT DESKTOP APPLICATION

Evidence Upload XT allows you to easily preview, annotate, and upload digital evidence to Axon Justice, ensuring secure access and comprehensive audit trails to track who uploaded files and when. Files in any format up to 1.6TB can be uploaded on a structured basis using flexible upload bandwidth settings.

/ API INGESTION

The API upload into Evidence.com allows seamless integration of external systems and applications to upload digital evidence directly into the platform. Using a standard API, organizations can automate the submission of files from third-party devices or systems, ensuring a smooth transfer of data without manual intervention. The process is simple, secure, and designed for high-volume uploads, enabling users to send evidence in bulk while maintaining chain-of-custody integrity. The API supports various file types and sizes, and once uploaded, the evidence is cataloged within Evidence.com with full audit trails to track submissions.

/ TRUSTED UPLOAD

Axon's Trusted Upload simplifies the process of transferring digital evidence by enabling justice customers to request evidence from trusted external partners, streamlining the entire request and submission workflow. Internal users can initiate a request directly within the system, specifying the required evidence and notifying external users via email. Recipients can then easily drag and drop the requested evidence into a centralized location, ensuring a smooth and efficient submission process.



/ AXON COMMUNITY REQUEST

Axon Community Request is a function designed to streamline digital evidence collection from the public. It offers distinct methods for gathering evidence from individuals or public portals seeking information from anyone who has relevant information.

- ▶ 1:1 invite are direct invitations to request a piece or pieces of evidence from a citizen.
- ▶ Community portals simplify mass evidence collection at events or incidents by allowing citizens to easily upload digital evidence via QR codes, social media links, or direct access.

/ AXON CAPTURE

Axon Capture is a mobile app that allows users to effortlessly capture photos, audio recordings, or videos using their mobile devices and upload them directly into Axon Justice. This seamless process ensures that evidence is securely stored and instantly made available for review, without the need for manual transfers or additional software.

/ AXON DATA MIGRATIONS

For larger or more complex data migrations, Axon's professional services team is available to help customers transfer significant data sets from source systems into Evidence.com. A scoping process is necessary to define the details of the migration. If this service is required, Axon will collaborate with you to establish the scope and provide an itemized cost estimate.

UNLIMITED EVIDENCE STORAGE AND SECURITY

Axon Justice offers straightforward, **unlimited cloud storage**. As one of the largest cloud storage providers in the world, Axon securely stores data of some form for nearly every public safety agency in the United States. With our unparalleled scale, we can provide significant cost savings to our customers, while eliminating the unpredictability of variable-rate storage contracts often seen with other vendors.

SUPPORTED FILE TYPES

Digital evidence comes in thousands of formats, many of them being extremely complicated to interact with and view. Axon Justice is source-agnostic, meaning it can support an almost unlimited range of file types, including proprietary and non-standard formats. This adaptability enables the Agency to effortlessly integrate existing systems and workflows into the interconnected Axon Ecosystem, amplifying the overall effectiveness of evidence management.

DEDICATED STORAGE FOR SENSITIVE CASE MATERIALS

Some cases require additional security controls, particularly those involving sensitive materials such as child exploitation evidence or protected witness testimony. Axon Justice offers dedicated storage instances that:



- ▶ Limit access to authorized personnel
- ▶ Support audit logs that track access and activity for compliance purposes.
- ▶ Help agencies align with privacy and legal requirements by isolating high-risk evidence from general case files in an entirely separate instance of Axon Justice for an extra layer of security.

MAINTAINING THE CHAIN OF CUSTODY

Tracking how digital evidence is handled throughout its lifecycle is critical for preserving case integrity and supporting legal workflows. Axon Justice helps agencies monitor and document every action taken on case materials, from ingestion through disclosure, by:

- ▶ Recording every interaction with evidence, including uploads, edits, shares, and access logs, in an automated audit trail.
- ▶ Maintaining tamper-resistant audit logs, which cannot be removed, even if a file or user is deleted, helping agencies retain a complete case record.
- ▶ Logging key metadata, such as SHA-2 hash values, timestamps, and file usage details, to help agencies verify file history and activity.
- ▶ Restricting access to evidence logs based on role-based permissions, ensuring only authorized personnel can view or generate audit reports.
- ▶ Providing exportable reports in PDF or CSV formats, allowing legal teams to review and filter case activity based on date ranges, user actions, and evidence status.

By automating chain-of-custody tracking and preserving an unaltered record of evidence activity, Axon Justice helps legal teams manage digital case materials with greater accountability and transparency.

SECURITY AND COMPLIANCE CONTROLS

With digital evidence playing a critical role in legal proceedings, agencies need a structured system to help protect case materials from unauthorized access and security threats.

Axon Justice is designed with an Information Security Program that includes:

- ▶ Access management and continuous security monitoring.
- ▶ Data encryption, classification, and controlled access settings.
- ▶ Risk management, vulnerability detection, and audit capabilities.

Additionally, Axon Justice aligns with industry security and compliance frameworks, including CJIS, FedRAMP, GDPR, ISO 27001, ISO 27017, ISO 27018, ISO 27701, HIPAA, and more. More details on Axon's world-class security can be found at axon.com/trust.



EVIDENCE PROCESSING AND REVIEW

The exponential growth of digital evidence affects the ability of legal teams to manually review and process evidence. Axon Justice integrates AI-powered automation to streamline the processing and analysis of video, audio, and document-based evidence, accelerating case preparation.

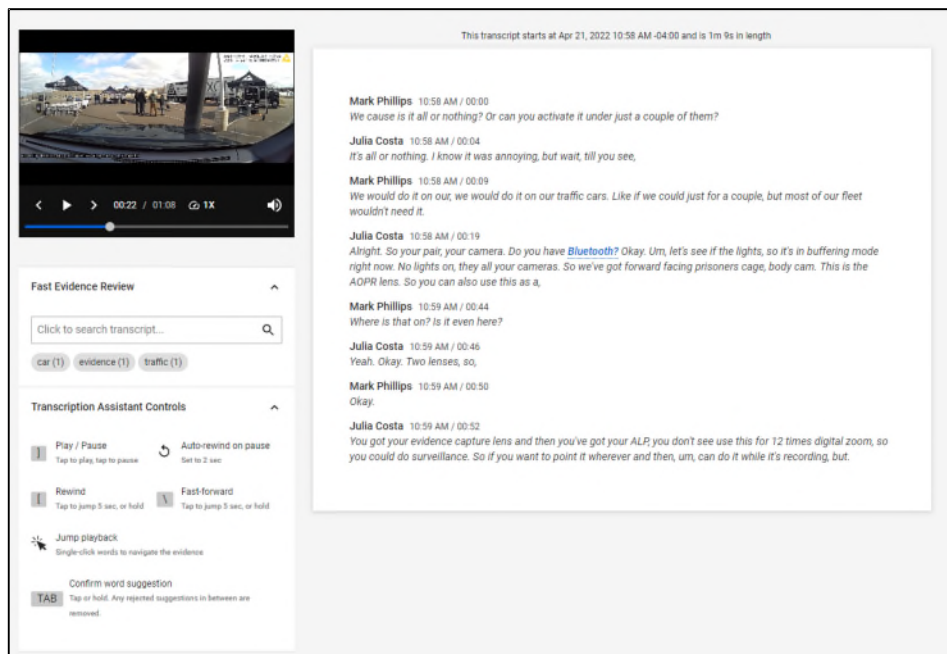


With automated transcription, redaction, summarization, and translation, Axon Justice enables attorneys to quickly search, review, and refine digital case materials while ensuring compliance and data security. These tools improve workflow efficiency, allowing legal teams to focus on case strategy rather than time-consuming evidence management.

AXON AUTO-TRANSCRIBE

Processing audio and video evidence manually is time-consuming and can delay critical casework. Axon Auto-Transcribe automates this process by generating accurate, time-synced transcripts that allow legal teams to search, analyze, and navigate digital evidence efficiently.

- ▶ **FASTER EVIDENCE REVIEW** – Convert up to 16 hours of recordings into audio-linked searchable text within 5 minutes.
- ▶ **SEARCHABLE TRANSCRIPTS** – Enables users to locate key words, phrases, or moments across a single transcript or multiple transcripts in seconds. Search results are linked to time stamps in the video to jump to the keyword in the record for playback.
- ▶ **TRANSCRIPT EDITOR** – Allows for quick refinements, making transcripts court-ready in less time.
- ▶ **INTEGRATED AUDIO REDACTION** – Users can redact specific words directly from the transcript, simplifying sensitive information handling.





AI REDACTION STUDIO

Redacting sensitive information in video and audio evidence is a necessary but time-consuming process. Axon Justice AI provides automated redaction tools that help legal teams efficiently remove confidential details while preserving evidence integrity.

- ▶ OBJECT AUTO-DETECTION – Identifies and tracks faces, license plates, screens, and other sensitive elements for redaction.
- ▶ AUDIO REDACTION VIA TRANSCRIPT – Allows users to mute words directly from the transcript, significantly improving workflow efficiency.
- ▶ AUTOMATED PROCESSING – Redactions continue running in the background, reducing manual labor.



“With Auto-Transcribe, I can get through the initial sweep of a case 25-50% faster, especially if it’s a video-intensive case.”

LISA BORDEN // ASSISTANT
DISTRICT ATTORNEY
ECTOR COUNTY, TEXAS



AXON BRIEF ONE

With video, audio, and documents making up a growing share of digital evidence, legal teams can be overwhelmed by the volume of materials they need to review. Manually analyzing hours of recordings or hundreds of documents can slow case preparation and increase the risk of overlooking key information.



Axon Brief One leverages AI-powered case summarization to help attorneys efficiently process large volumes of digital evidence, generating structured overviews that highlight the most critical case elements. Instead of sifting through raw files, legal teams receive a clear, AI-generated summary, enabling faster evidence review, decision-making, and trial preparation.

- ▶ **EVIDENCE SUMMARIZATION**—Automatically review succinct summaries on every piece of evidence with an audio track, to efficiently review evidence in charging decisions and make decisions on where to spend valuable time. OCR expected end of 2025, with summarization to be expanded into txt, word, and pdf files.
- ▶ **KEY MOMENT IDENTIFICATION** – Flags important video or audio segments, allowing users to quickly locate crucial case details.
- ▶ **SUMMARIZATION** – Aggregate key details from individual pieces of digital evidence into a full case synopsis, making it easier to identify what data needs attention.
- ▶ **KEY MOMENT IDENTIFICATION** – Flags important video or audio segments, allowing users to quickly locate crucial case details.
- ▶ **CASE QUERYING** – Query function within a case to ask pertinent questions and help sift through case materials.

EVIDENCE TRANSLATION

As legal cases increasingly involve multilingual evidence, language barriers can delay case progress, complicate discovery, and increase reliance on costly external translation services. Reviewing foreign-language interviews, transcripts, and documents manually requires additional resources.

Axon Justice AI provides real-time, automated translation, enabling legal teams to efficiently review and share multilingual evidence without the need for third-party translators or time-consuming manual transcription. By converting foreign-language evidence into searchable, English-translated transcripts, attorneys can quickly analyze key details, cross-reference materials, and ensure comprehensive case preparation.

- ▶ **MULTI-LANGUAGE SUPPORT:** Translates AI-generated transcripts into 57+ languages (with more being added regularly).
- ▶ **REAL-TIME TRANSLATIONS:** Provides instant, accurate translations of digital evidence, minimizing delays.
- ▶ **AI-DRIVEN ACCURACY:** Maintains the integrity and context of original transcripts for precise communication.



- ▶ **FASTER CASE PREPARATION:** Speeds up the process of preparing cases by eliminating the need for manual translations, saving time and resources.
- ▶ **COST-EFFICIENCY:** Reduces reliance on expensive translation services, lowering overall case management costs.

ADVANCED CASE ORGANIZATION

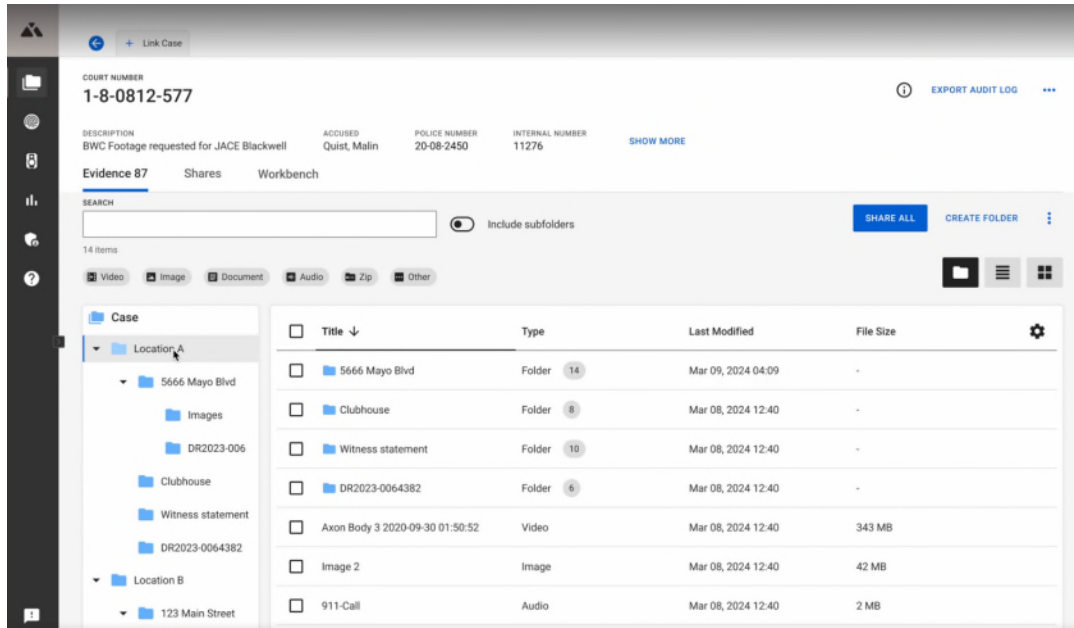
Legal professionals across the U.S. have consistently expressed the need for a more structured, Windows-style foldering system for managing digital evidence within Axon Justice. While our current system utilizes a tagging and categorization approach, we recognize that many legal teams are accustomed to working with traditional hierarchical folder structures when organizing case materials.

To address this feedback, we have developed a new enhanced foldering tool, designed to provide a more intuitive and efficient way to manage evidence. This enhancement will allow prosecutors, defense attorneys, and legal staff to organize files in a way that mirrors their existing workflows, making it easier to locate, review, and present case materials.

- ▶ **Familiarity & Ease of Use** - Legal teams can organize digital evidence using a folder-based approach similar to Windows Explorer, reducing the learning curve and improving adoption rates.
- ▶ **Improved Case Organization** - Attorneys can create, name, and arrange folders in a way that aligns with their specific case structures, streamlining case management.
- ▶ **Faster Evidence Retrieval** - A more structured foldering system means less time spent searching for critical files, allowing legal professionals to focus on case strategy rather than document management.
- ▶ **Seamless Transition & Integration** - This enhancement integrates seamlessly with existing Axon Justice features, ensuring that both tagging and structured foldering options remain available to accommodate different user preferences.
- ▶ **Scalability for Large Cases** - High-profile and complex cases often involve thousands of digital files. The enhanced foldering system will significantly improve document handling, making it easier to manage extensive evidence collections.



New Case Organization interface:



ADVANCED CASE SEARCH

Managing criminal cases for Prosecutors or Defense Attorneys often involves reviewing thousands of pages of PDFs, extensive audio and video recordings, and vast amounts of case-related data. Traditionally, locating specific details within this massive volume of digital evidence has been a time-consuming and labor-intensive process. Prosecutors, investigators, and defense attorneys are often forced to conduct multiple searches across different platforms, manually sift through documents, and rely on limited keyword indexing—slowing down investigations and case preparation.

To address these challenges, Axon Justice is introducing a powerful new search capability that extends beyond the existing in-case search functionality. This advanced search engine enables legal professionals to:

- ▶ **Search Within PDFs** - Many critical case documents—including police reports, forensic analysis, and legal filings—are stored as rich-text PDFs. Our enhanced search feature will index and extract text from these documents, allowing attorneys to quickly pinpoint specific phrases, names, or case details.
- ▶ **Search Transcripts from Video & Audio Files** - Reviewing recorded interviews, interrogations, body-worn camera footage, and wiretap recordings is often a slow and resource-intensive task. With our automated transcription technology, attorneys can now search within text-based transcripts of these recordings, making it easier to locate key statements, admissions, or inconsistencies in witness accounts.
- ▶ **Universal Case-Wide Search** - Instead of manually searching through separate files, media, and case documents, users can conduct a single, consolidated search across all case materials. This includes searching through emails, case notes, call logs, and evidence descriptions—ensuring no critical detail is missed.



VIDEO PLAYBACK, EDITING, AND EXHIBIT CREATION

Historically, the process of transforming vast amounts of digital evidence into digestible, court-ready exhibits for presentation to a jury has been a labor-intensive and error-prone task. Prosecutors and defense attorneys were often required to download raw data, import it into third-party applications, master complex video editing tools, export the files, and then re-upload them to share with opposing counsel and the court. This multi-step process was not only time-consuming, but also introduced significant risks, including data loss, corruption, and inconsistencies.

Axon Justice fundamentally redefines this workflow by offering a suite of professional, intuitive tools specifically designed for the needs of prosecutors and defense attorneys. With Axon Justice, users can seamlessly review, edit, and present digital evidence directly within the platform, without the need for external software or complex processes.

VIDEO EDITING

Key features include advanced editing functions like cutting and clipping, which allow users to extract relevant segments of video without altering the original file. For cases requiring seamless continuity, the stitching tool enables the combination of multiple video files into a single cohesive clip. Additionally, users can easily bookmark critical moments within a video, helping to highlight key evidence for quick access and presentation. These powerful, easy-to-use tools empower legal professionals to manage and present video evidence with efficiency and precision, all while maintaining the integrity of the original content.

MULTI-CAM

Axon Justice's Multi-Cam function revolutionizes the way video evidence is presented by seamlessly time-syncing video from multiple Axon devices, including Body-Worn Cameras (BWC) and Fleet In-Car Video Systems. This powerful tool allows users to playback up to four video streams simultaneously, providing a comprehensive, multi-angle view of critical events. For enhanced courtroom presentations, Multi-Cam also enables the export of a single unified file containing all four video streams, creating a cohesive and immersive demonstrative. This feature offers juries unparalleled situational awareness, allowing them to experience the scene from multiple perspectives and gain a more complete understanding of the events in question. Whether used for case review or courtroom presentation, Multi-Cam enhances clarity, strengthens arguments, and significantly improves the impact of video evidence.

THIRD-PARTY VIDEO SUPPORT

The third-party video playback feature allows users to play videos not natively supported by the default video player. With this feature when a proprietary video format is uploaded, the system will automatically begin converting the file to MP4 so it can be viewed within Axon.



Justice. The original video will remain unchanged in its original format and will be maintained in the system together with the converted video which can be played, transcribed, redacted, and managed in Axon Justice.

The system currently supports approximately 93% of available video codecs, helping legal teams review digital evidence from the cloud without compatibility concerns. Our proprietary or exotic files extension list is constantly growing as we work to add support for new file formats and their variations.

If a file in an unsupported format is found, users can contact support@axon.com to request that it be added at no cost to the user. For a complete list of supported file types see Appendix A.

AXON INVESTIGATE

Axon Investigate is the most advanced video editing tool that we provide as a part of Axon Justice. It protects truth by providing an intuitive interface that unlocks the power of video evidence in an efficient, forensically sound manner.

- ▶ **TESTIFY WITH CONFIDENCE** – Users can bring Axon Investigate into the courtroom and play full screen, zoomed or looped video evidence for the trier of fact while on the stand.
- ▶ **ORGANIZE VIDEO INVESTIGATIONS WITH AXON INVESTIGATE** – Users can bring together video from multiple sources, organize clips into groups, visualize stationary and moving cameras on a map, generate Court packages, attach content warnings, and categorize metadata to uncover the full story by leveraging easy filter, sort and search functions.
- ▶ **MAP EVIDENCE** – Users can visualize stationery and moving cameras on a map with coordinate information to build cases around multiple cameras, locations and moving people
- ▶ **ENHANCE** – Users can enhance images and video to provide additional clarity to important evidence. Uncover hidden information in video images with powerful and easy-to-use clarification tools.
- ▶ **CAMERA MATCH OVERLAY** – Investigators can accurately calibrate and overlay video and imagery onto 3D point cloud data. Users can determine positions, distances, heights and other key measurements with their native 3D scanning software.
- ▶ **TRAINING AND CERTIFICATION** – Innovative live and online training courses take a hands-on approach to teaching best practices for handling video evidence. Participants receive virtual access to case files; an Axon Investigate instance and a live trainer.

Additional information is available at axon.com/products/axon-investigate.

ZIP FILE PREVIEW

The Zip Preview feature in Axon Justice significantly streamlines the process of managing and reviewing compressed files, enhancing both efficiency and ease of use. This feature allows users to preview the contents of a ZIP file directly within the Axon Justice platform without the need to download, extract, and re-upload the file. By eliminating these extra steps, Zip Preview saves valuable time and reduces the risk of errors or file mismanagement.



Additionally, Zip Preview enables the native extraction of files within the system, further simplifying the workflow. Users can quickly access and interact with individual files contained within the ZIP archive without leaving the Axon Justice platform, ensuring a more seamless and organized process.

CASE ROUTING, NOTIFICATIONS, AND ACCESS CONTROL

Centralizing evidence in a single system does more than simply centralize the intake and management of evidence. It streamlines the ability of legal teams to handle complex casework by ensuring that evidence access, case building, routing, notifications, and security controls are seamlessly integrated into a single, intuitive platform.

Axon Justice eliminates the inefficiencies of fragmented systems by consolidating all case-related functions in one place, reducing administrative burdens and improving workflow efficiency. With a unified interface, attorneys can efficiently search, review, and organize evidence, while automated routing, real-time notifications, and role-based access controls ensure secure, compliant, and seamless collaboration from intake to resolution.

CASE ROUTING WORKFLOWS & NOTIFICATIONS

With digital evidence structured and readily available, Axon Justice seamlessly transitions cases into automated workflows with real-time notifications, ensuring they reach the right team members at the right time. Axon Justice enables configurable case routing, ensuring that cases move seamlessly from initial submission to final resolution. Based on predefined criteria and metadata, cases can be automatically assigned for initial review before being directed to the appropriate counsel and support staff. This eliminates manual handoffs, reduces delays, and ensures cases reach the right team members at the right time.

Automated notifications keep all stakeholders informed throughout the case lifecycle. As cases progress—from intake to assignment, review, and final disposition—attorneys, support staff, and intake teams receive real-time alerts when evidence is submitted, or key actions occur. This ensures continuous visibility, reduces oversight risks, and improves team coordination.

CUSTOM CASE METADATA

Supporting this structured workflow, custom case metadata enhances searchability and organization, allowing users to categorize cases based on court numbers, case status, assigned personnel, and other relevant details. Attorneys can quickly filter and retrieve case materials, while administrators can enforce standardized data entry using field validation and predefined formats. This integration of custom metadata, automated case routing, and real-time notifications ensures legal teams have a cohesive, efficient, and fully trackable case management process. Cases in Axon Justice can include metadata in several editable fields, including:

- ▶ **COURT NUMBER** – An optional freeform alphanumeric field indicating the court or docket number of the case. A single number can be entered.



- ▶ DESCRIPTION – An optional freeform alphanumeric field that allows users to enter a description of the case.
- ▶ POLICE NUMBER – A mandatory freeform alphanumeric field indicating the police-given number of the case. A single number can be entered.
- ▶ ACCUSED – An optional freeform alphanumeric field indicating the accused party's name. Multiple names can be entered into this field.
- ▶ CASE STATUS – An optional dropdown list that allows users to select from Active, Dismissed, Plea Bargained, Tried (Lost), and Tried (Won) case statuses.
- ▶ TAGS – Optional freeform alphanumeric labels that can be applied to cases. Adding tags can help to search and sort cases. For example, users may enter the name of the assigned judge or prosecutor, the charges in question, or any other terms that will help search in the future.
- ▶ CASE OWNER – This field searches all active users in an Axon Justice account, allowing users to reassign a case if needed.
- ▶ CASE RETENTION – An optional dropdown list that allows users to select from available case retention policies: Specific Date, Longest Retention Period, Until Manually Deleted, or Individual Evidence Retention.

Additionally, administrators can use the Field Validation feature to ensure that users enter information in your office-defined format for specific fields. Administrators can develop a regular expression (regex) entry to set the required format for the police number, court number, and internal number fields in Axon Justice.

ACCESS CONTROL, ACTIVE DIRECTORY, AND SSO

Beyond streamlining evidence ingestion, centralizing case-building and sharing in Axon Justice enhances security, access control, and compliance, ensuring that sensitive case materials remain protected at every stage. By enforcing role-based permissions, centralized authentication, and auditable access tracking, Axon Justice helps agencies align with legal, regulatory, and cybersecurity requirements, safeguarding digital evidence while maintaining operational efficiency.

ROLE-BASED ACCESS CONTROL (RBAC) & COMPLIANCE

Role-Based Access Control (RBAC) enforces strict user permissions, ensuring personnel only view, edit, or share case materials relevant to their responsibilities. By defining clear, role-based security policies, Axon Justice prevents unauthorized access, reduces compliance risks, and ensures chain-of-custody integrity. Additionally, RBAC strengthens compliance by automating access tracking and audit logging, ensuring that all user actions, case file interactions, and evidence modifications are documented, time-stamped, and aligned with legal and regulatory mandates.

ACTIVE DIRECTORY AND SINGLE SIGN-ON

Axon Justice integrates Active Directory (AD) and Single Sign-On (SSO) to enhance security, streamline access, and ensure compliance with CJIS, ISO, and other security standards. With Active Directory, agencies can centrally manage user accounts, roles, and permissions, eliminating manual account creation and reducing administrative workload.



Single Sign-On (SSO) enables users to access Axon Justice and connected systems with a single, authenticated login, reducing reliance on weak or reused passwords and ensuring uniform authentication policies across all integrated platforms. By enforcing multi-factor authentication (MFA) where required and maintaining audit logs of login activity, SSO strengthens access security, prevents unauthorized entry, and ensures compliance with legal and cybersecurity mandates.



DISCOVERY AND EXTERNAL SHARING

Axon Justice transforms the discovery process for both prosecution and defense by providing a streamlined, secure, and efficient platform for evidence sharing and access. The primary method of discovery is through a dedicated, no-cost disclosure portal, giving defense attorneys secure, on-demand access to evidence shared by the prosecution.

Beyond standard discovery between prosecution and defense, additional sharing is often required, whether with expert witnesses, medical examiners, or the court. With a suite of powerful tools, Axon Justice ensures that users can seamlessly share evidence with all the necessary partners.

DISCLOSURE PORTAL

Axon Justice simplifies and streamlines the discovery process by providing a dedicated disclosure portal for defense attorneys, at no cost to them. This secure, user-friendly portal allows defense teams to log in and access discovery that has been shared by the prosecution. Once logged in, attorneys can easily view and download evidence directly from the portal, offering complete flexibility in how they manage and store the files.

EMAIL DOWNLOAD LINKS FOR EXTERNAL USERS

Axon Justice also provides a simple and efficient method for sharing evidence via email download links. Users can easily send a download link to any email address, allowing recipients to access a zip file containing the shared evidence. This straightforward process ensures that evidence can be quickly and securely transferred to individuals who may not have direct access to the system, such as expert witnesses or external partners.

COURT PACKAGE EXTRACT

The Axon Court Package Extract allows users to easily create a complete package of evidence for submission to court. This tool is designed for jurisdictions that require physical copies of digital evidence. With just a few clicks, users can extract and compile evidence directly from the system, ensuring a streamlined process for court submissions while maintaining the integrity and organization of the evidence.

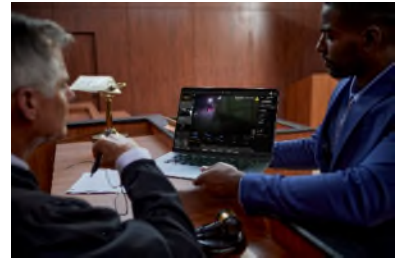
DISCLOSURE LOG

Axon Justice enhances transparency and accountability in the discovery process by automatically generating a detailed PDF "Disclosure Log." This log provides a comprehensive record of all evidence shared via the Axon Disclosure portal with opposing counsel. It includes a clear, itemized list of each evidence file, the individuals it was sent to, and the exact timestamp of when the files were shared, all derived from the system's robust audit trail. This ensures full compliance with legal disclosure requirements and helps attorneys quickly confirm the evidence provided. The Disclosure Log acts as a powerful tool for both legal teams and the court, offering an easy-to-access, verifiable record of discovery exchanges and safeguarding against any disputes or questions regarding the timeliness or completeness of shared evidence.



THIRD-PARTY SYSTEM INTEGRATIONS

Axon Justice further enhances legal workflows by integrating with existing 3rd party systems to provide greater access to evidence from more places. Axon Justice has been built with an extremely robust integrations platform leveraging a comprehensive set of APIs. With this integration platform users have an endless opportunity to integrate the power of Axon Justice into other systems.



CELL PHONE EXTRACTION VIEWER (COMING 2026)

Mobile forensic evidence, especially cell phone extractions, often come in complex formats that require specialized software for review. Axon Justice simplifies this by enabling agencies to manage these files directly within their case workflow.

- ▶ SEAMLESS CELL PHONE EXTRACTION FILE UPLOAD – UFDR files can be uploaded directly into Axon Justice or transferred through Axon Partner Share, helping agencies manage mobile forensic evidence more effectively.
- ▶ INTEGRATED READER – Investigators and attorneys can review mobile device data within Axon Justice, eliminating the need for additional software.
- ▶ AI-POWERED REVIEW TOOLS – Transcription, search, and filtering tools help identify relevant messages, call logs, and multimedia files.
- ▶ CROSS-TEAM COLLABORATION – Mobile evidence can be shared between law enforcement, prosecutors, and defense attorneys, helping to support legal discovery and review.

By integrating a cell phone extraction viewer into Axon Justice, agencies can manage mobile forensic evidence within a structured digital case workflow.

CASE MANAGEMENT SYSTEM (CMS) INTEGRATION

Legal professionals rely on CMS to track case progress, manage filings, and organize case-related records. By integrating digital evidence directly into CMS platforms, Axon Justice ensures that all case-related materials are securely tracked and linked, reducing the risk of misplaced evidence and maintaining an auditable chain of custody. Every interaction with evidence is automatically recorded, helping legal teams comply with disclosure rules, public records laws, and judicial transparency requirements.

- ▶ SINGLE-PLATFORM ACCESS – The goal of this integration is to bring files from both systems into one place without replicating the data, which would be costly for agencies. With the Axon Justice API's, data can be stored in Axon Justice while being linked into CMS for viewing.
- ▶ AUTOMATED CASE LINKING – Evidence uploaded to Axon Justice is associated with the correct case, keeping files categorized and easy to locate.
- ▶ AUDIT TRAILS AND COMPLIANCE – Every evidence interaction is documented in an audit log, helping legal teams track chain-of-custody activity and maintain case organization.



By connecting case records with digital evidence, Axon Justice helps legal teams streamline case management and improve collaboration across departments.

TRIAL PRESENTATION SOFTWARE INTEGRATION

Presenting digital evidence in court is a key component of legal proceedings, and manual processes for preparing exhibits can increase workload and delay trials. Axon Justice integrates with third-party trial presentation software, allowing legal teams to prepare and present case materials more efficiently.

- ▶ **DIRECT EVIDENCE EXPORT** – Case files and digital evidence can be transferred to courtroom presentation systems without manual downloads or file conversions.
- ▶ **FORMAT STANDARDIZATION** – Helps legal teams prepare court-ready materials, reducing the risk of formatting issues or missing files.
- ▶ **WORKFLOW EFFICIENCY** – Attorneys can review and structure evidence before presentation, helping to build a clear, organized case narrative.

This integration helps simplify courtroom preparation, allowing legal teams to focus on case strategy rather than file logistics.



AXON JUSTICE HARDWARE ADD-ONS

Axon Justice is more than a digital evidence management system—it serves as the central hub for agencies using Axon’s comprehensive suite of hardware devices, creating a fully integrated evidence ecosystem. By seamlessly connecting evidence collection, storage, and case management, agencies reduce dependency on external submissions, improve chain-of-custody integrity, and accelerate case preparation.

AXON BODY-WORN CAMERAS

A body-worn camera system is a wearable recording device that captures high-quality video and audio, allowing investigators to document interviews, witness statements, and other case-related interactions in real time. Unlike standalone recording devices, Axon body-worn cameras can automatically upload footage to Axon Justice. Many Prosecution or Defense investigators across the US are using Axon Body worn Camera’s for video collection.



AXON INTERVIEW ROOM SYSTEMS

An interview room system is a fixed recording setup specifically designed for legal and investigative settings. These systems capture high-quality video and audio recordings of interviews, witness statements, and interrogations while ensuring secure storage, structured access, and easy retrieval for case preparation.



Axon Interview is a comprehensive, purpose-built interview room solution that provides:

- ▶ **HIGH-QUALITY RECORDING** – Captures clear, courtroom-ready video and audio evidence.
- ▶ **MULTI-CAMERA VIEWS** – Supports covert, dome, and PTZ cameras for different room setups.
- ▶ **AUTOMATED RECORDING CONTROLS** – Includes motion-based triggers and touch-panel controls to start and manage recordings easily.
- ▶ **CONTINUOUS REDUNDANCY** – Uses dual-server storage to help maintain secure and accessible recordings.

INTEGRATION WITH AXON JUSTICE

Once an interview is recorded, Axon Interview automatically uploads the file to Axon Justice, helping agencies eliminate manual file transfers and reduce administrative workload. From within Axon Justice, legal teams can:

- ▶ Auto-transcribe recordings into searchable, time-synced transcripts.
- ▶ Review and annotate interviews directly within the case file.
- ▶ Apply redactions to protect sensitive information before discovery or trial.
- ▶ Securely store, access, and share recordings with relevant stakeholders.



AXON JUSTICE DEPLOYMENT PROCESS

Axon's Software Services (SWSS) team provides comprehensive implementation services and training to help our Justice partners adopt and integrate our technologies seamlessly. Our experienced deployment team works closely with your office to provide tailored training and implementation support, to help with a seamless adoption process which meets your specific needs.

PARTNERING WITH AN EXPERIENCED TEAM

Axon's SWSS team has extensive experience helping agencies of all sizes implement their DEMS programs. Our solution, specifically developed with our Justice partners in mind, along with customizable deployment plans and an experienced deployment team, make Axon uniquely positioned to provide Client with effective deployment, training, and support services. With Axon's staff managing your installation, Client can expect project alignment that gives end users a thorough understanding of the solution's features and functionality.

This combination of deployment expertise and tailored support helps reduce onboarding time and can improve end-user adoption rates. Many of our SWSS team members have past experience in the law enforcement or Justice sectors, where they were responsible for planning and managing projects similar to those they now help deploy. This allows them to anticipate challenges unique to these environments, collaborate effectively with command and IT staff, and provide solutions tailored to your needs. Our staff can also offer guidance on custom workflows and processes to help Client use your DEMS effectively and in compliance with local laws and statutes.

PHASES OF THE PROPOSED PROJECT PLAN

We've built the proposed project plan to reflect lessons learned in our many past successful deployments. To provide the basic structure needed for a deployment, plans are split into the following phases:

- ▶ **INITIATION** – Establishes key points of contact, deployment expectations, and project kickoff planning.
- ▶ **PLANNING** – Configures test environments and reviews agency workflows to tailor the implementation.
- ▶ **CONFIGURATION** – Finalizes system settings, security controls, and ingest/disclosure portal configurations.
- ▶ **TRAINING** – Provides end-user training to ensure legal teams can fully utilize Axon Justice.
- ▶ **GO-LIVE** – Validates system functionality, executes final testing, and transitions to active use.
- ▶ **Integrations** – After the system is up and running, we will work to advise on the integrations of Axon Justice into 3rd party systems.
- ▶ **HANDOVER** – Transfers ongoing support to Axon's Customer Success and Technical Support teams.



Each phase is made up of individual activities which will be adapted to your specific deployment objectives and products purchased. Further details on the activities, deliverables, and timelines for the phases are provided in the following sections.

INITIATION PHASE

The initiation phase begins once Axon has been selected as your preferred vendor and contract documents have been negotiated and signed. Your account will be handed off by your account executive to our SWSS team, who will begin the deployment introduction and planning process.

Client should designate a main point of contact within your office to serve as the client project coordinator. This person will coordinate discussions and meetings between Client and Axon and will work directly with our team to ensure a smooth deployment and training process.

Additionally, your office should identify system administrators and power users—those who will use the system most frequently. Any law enforcement partners who are not current Axon customers should also be identified, as ingest portals may need to be created for them during the deployment. If data migration is required, your IT staff may also need to be involved in the deployment process.

PLANNING PHASE

During the planning phase, the BA will set up and provision test sites, including an Axon Justice test site and test disclosure and ingest portals. Links to the test sites will be given to your designated Axon Justice administrator who can add any needed users. The deep-dive and administrator calls will take place.

CONFIGURATION PHASE

The configuration phase involves finalizing the setup of Axon Justice in preparation for training and go-live. This includes Axon's internal teams creating the necessary ingest and/or disclosure portals and providing you with materials to be given to your partners for training on the new processes. This can also include any final adjustments that Client may want to make to roles and permissions prior to team trainings.

TRAINING PHASE

With the system configured, the project can move into the training phase. Our proposal includes virtual training for end-users.

Our goal is for your staff to leave with a working understanding of Axon Justice and readiness to use it effectively in their role. The content of the training sessions will be tailored to your needs as discussed during the deep-dive call. A proposed agenda can be sent prior to the training sessions for review. Pre-work may be required to ensure sessions are as productive and interactive as possible.

Materials will be provided, which can be provided to your law enforcement partners for training on the new evidence intake procedures.



GO-LIVE PHASE

The go-live phase marks the final deployment step in which Axon Justice becomes fully operational. Prior to go-live, the BA performs system testing and validation to ensure proper configuration. The Axon BA will also work with your office to schedule the go-live date; this is typically executed during off-hours or over a weekend to minimize any potential disruption to operations. The BA can also work with you to draft end-user communications regarding the launch of Axon Justice.

Note that if Axon-assisted data migration is a part of your deployment, a separate timeline and project milestones will apply and may be ongoing at the time of go-live.

HANDOVER PHASE

Together, Client and Axon will conduct a final system review and sign paperwork which certifies completion of the deployment. Once the paperwork is signed, the deployment is considered officially complete and ongoing account management will be handed over to the following teams.



OUR EXPERIENCE



For more than three decades, Axon has been developing technology for public safety, providing agencies with the tools needed to capture, manage, and share digital evidence. Founded in 1993, Axon initially focused on hardware solutions like TASER energy weapons and body-worn cameras before expanding into cloud-based evidence management to

support digital casework.

As digital evidence collection surged across public safety agencies, Axon recognized that storing, managing, and organizing vast amounts of data required a scalable solution. This led to the development of Axon Evidence in 2009, a cloud-based DEMS that allowed agencies to store, organize, and manage growing volumes of digital case materials. Today, Axon Evidence serves more than 1,000,000 cumulative users worldwide, including law enforcement, investigators, and legal professionals, making it the most widely adopted DEMS in public safety.

While Axon Evidence helped law enforcement centralize digital files, it became clear that prosecutors and defense attorneys needed easier access to this evidence. To address this, Axon developed the Axon for Prosecutors Program (APP), a web-based case-building site within Axon Evidence, allowing legal teams to efficiently receive and organize digital evidence for discovery and case preparation.

As justice users required more specialized tools and workflows than their public safety counterparts, Axon built Axon Justice, one of the industry’s first DEMS designed specifically for legal professionals. This provided dedicated dashboards, evidence review tools, and automated discovery workflows to support prosecutors, defense attorneys, and court officials.

“With Axon Justice, we made sure that we were able to utilize unlimited storage, because we recognized we weren’t only going to have Axon evidence, but other types of digital evidence that we’d need to ingest from non-Axon users. We then were able to leverage the true power of Axon Justice Premier, that is things like transcription, seeing when our lawyers or individuals in the department have reviewed pieces of evidence or when they haven’t, delivery to public defenders or the probation department. It became a significant game changer for us.”

MIKE FERMIN // CHIEF ASSISTANT
DISTRICT ATTORNEY

SAN BERNARDINO COUNTY
DISTRICT ATTORNEY’S OFFICE

APPENDIX



APPENDIX A

THIRD-PARTY VIDEO SUPPORTED FILE TYPES

Axon's Third-Party Video feature supports playback for thousands of formats, many of which are proprietary and don't have known names. Our engineering team builds support for new formats every week, based on customer requests.

Note that a file format is not the same as a file extension, and that a file extension doesn't necessarily identify the format. Additionally, file extensions (such as .avi, .mp4, .dav, and .exe) can be used with multiple types of formats. This document lists the extensions most often used to name our supported formats.

Axon supports playback of most file formats from many video manufacturers, including Airship, Apollo Video, Avigilon, Bosch, Cathexis, ClickIt, Dahua, DepotView, Digital Watchdog, DVTel, EverFocus, ExacqVision, Eyeonenet Backup, Eyesight IP, For the Record, Flir, Fuho Technologies, Genetec, Geovision, Go-Pro, GTL, Hikvision, Honeywell, ID View, Interlogic, IRoad, Janus, Kroger Brand Stores, L3 Mobile, Liberty, LiveView Technologies, Lorex, Magic Series, March Networks, Milestone, Night Owl, Obseron, Ocularis, Origin Lab, Orion, Panasonic, Pelco, Q-See, QuickTime, Revo, Rosco Vision, Samsung, Seon, Smart Witness (aka SmartView), Swann, Synectics, Time Space Technology, TSI NexView, Verint, Wavestore, and WiseNet.



A	.acm, .aira, .aJp, .amr, .arv, .asd, .asf, .ass, .audio, .audioO, .audiol, .audio2, [...], .av, .av3, .ave, .avcl, .avd, .ave, .avi, .avr, .avs, .ax	N	n3r, .nis, .nmf, .nov, .nvf, .nvr, .nvt3
B	.bin, .bix, .blk, bmp, .bnk, .box, .bu, .BUP, .bvr, .bwv	O	o3r, .ocx, .ogg, .omc, .opus
C	.caf, .car, .cda, .cdf-ms, .eel, .chm, .CL4, .cme, .CR2, .cva, .eve, .cx3	P	par, .pef, .pes, .pie, .PNG, .ps, psf, .psx
D	d, .dad, .dar, .dat, .data, .dav, .davl, .dax, .db2, .DBF, .dee, .dcr, .dga, .dgv, .divx, .dmd, .dmi, .drv, .ds2, .DSS, .dv, .dv4, .dv5, .DVM, .dvr, .dvrlib, .dvs, .dvt, .dxa	Q	.qbx, .qtr, qtx
E	enc, .evf, .exe, .exo, .exp	R	raw, .red, .re4, .REC, .rem, .rf, .rm, .rms, .rmv, .rrsc, .rt4, .rw2, .rwv
F	.f4v, file, .FL4, fls, .flv	S	.s, .sec, .sfk, .sidx, .sjpg, .sm, .smi, .sng, .snx, .spx, .srt, .ssa, .ssf, .str, .STU, .swf, .synav
G	g64, .g64a, .g64m, .g64x, .gbf, .gif	T	.tdb, tfs, .THM, .thumb, tif, .tiff, .TL2, .TMP, .tn3, .tree, trm, .tr2, .trs, ts, .tts
H	.h264, .h265, .h3r, .h4v, .h64, .hav, .hbox, .hdv, .HEIC, .hik264, .hldvr, .his, .hrf	U	.umv
I	IFO, .ifv, .img, .index, .irf, .iso, .iva, .ivf	V	.vl7, .vl9, .V21, .V22, .V23, .v24, .v264, .vac, .vam, .vcl, .vid, .video, .videol, .video2, .video3, [...], .vision, .VL4, .VOB, .vs2, .vtt, .vvf
J	JDR, jfif, JPE, jpeg, .jpg	W	.wav, .wbr, .webm, .webp, .wgva, .WMA, .wmv, .wsb, .wva
K	kds, .keep, .ktx, .kvf	X	xba, xesc, .xll, .xpa
L	.164, .lnk, .lnr, .log, .LRV, .lvf, .lwx, .lxa	Y	N/A
M	.m2ts, .m2v, m4a, .m4v, .mdl, .mdt, .media, mjp, .mjpeg, .mjpg, .mkv, .MOV, .mp2, .MP3, .mp4, mpeg, .mpg, .mpg2, MPV, .mpvc, .mt9, .MTS, mxf, mxg	Z	.zip

CAPTURE TRUTH
ACCELERATE JUSTICE
PROTECT LIFE



Exhibit B

Axon Quote Q-810611-46108MK

Q-810611-46108MK
Issued: 03/27/2026

Quote Expiration:

Estimated Contract Start Date: 07/01/2026

Account Number: 486241
 Payment Terms: N30 Mode of
 Delivery: AUTO-GND Credit/Debit
 Amount: \$0.00

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



SALES REPRESENTATIVE	PRIMARY CONTACT
Molly Kinsella Phone: 4808055496 Email: mkinsella@axon.com Fax:	Sarah Hacker Phone: (559) 582-0326 Email: sarah.hacker@co.kings.ca.us Fax:

SHIP TO	BILL TO
Kings County District Attorney- CA- 1400 W Lacey Blvd Hanford, CA 93230-5905 USA	Kings County (CA) District Attorney 1400 W Lacey Blvd Hanford, CA 93230-5905 USA Email:

Discount Summary

Average Savings Per Year	\$185,882.40
TOTAL SAVINGS	\$1,858,824.00

Quote Summary

Program Length	120 Months
TOTAL COST	\$1,148,424.00
ESTIMATED TOTAL W/ TAX	\$1,148,424.00

Payment Summa

Date	Subtotal	Tax	Total
Jul 2026	\$109,403.96	\$0.00	\$109,403.96
Jul 2027	\$98,180.11	\$0.00	\$98,180.11
Jul 2028	\$102,107.32	\$0.00	\$102,107.32
Jul 2029	\$106,191.61	\$0.00	\$106,191.61
Jul 2030	\$110,439.28	\$0.00	\$110,439.28
Jul 2031	\$114,856.85	\$0.00	\$114,856.85
Jul 2032	\$119,451.12	\$0.00	\$119,451.12
Jul 2033	\$124,229.16	\$0.00	\$124,229.16
Jul 2034	\$129,198.33	\$0.00	\$129,198.33
Jul 2035	\$134,366.26	\$0.00	\$134,366.26
Total	\$1,148,424.00	\$0.00	\$1,148,424.00

Quote Unbundled Price: \$3,007,608.00
 Quote List Price: \$1,303,008.00
 Quote Subtotal: \$1,148,424.00

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									
S00031	JUSTICE PREMIER PLUS PLAN	60	120	\$415.64	\$178.89	\$157.42	\$1,133,424.00	\$0.00	\$1,133,424.00
A la Carte Services									
100491	AXON JUSTICE - PSO - STANDARD DEPLOYMENT	1			\$15,000.00	\$15,000.00	\$15,000.00	\$0.00	\$15,000.00
Total							\$1,148,424.00	\$0.00	\$1,148,424.00

Delivery Schedule

Software

Bundle	Item	Description	QTY	Estimated Start Date	Estimated End Date
JUSTICE PREMIER PLUS PLAN	100165	AXON EVIDENCE - STORAGE - THIRD PARTY UNLIMITED	60	07/01/2026	06/30/2036
JUSTICE PREMIER PLUS PLAN	101866	AXON BRIEF ONE FOR JUSTICE	60	07/01/2026	06/30/2036
JUSTICE PREMIER PLUS PLAN	101905	POLICY CHAT	60	07/01/2026	06/30/2036
JUSTICE PREMIER PLUS PLAN	101966	AXON UNLIMITED SMART DETECTION	60	07/01/2026	06/30/2036
JUSTICE PREMIER PLUS PLAN	102525	MOBILE DEVICE EXTRACTION VIEWER	60	07/01/2026	06/30/2036
JUSTICE PREMIER PLUS PLAN	102610	AXON COMMUNITY LINK	60	07/01/2026	06/30/2036
JUSTICE PREMIER PLUS PLAN	73478	AXON EVIDENCE - REDACTION ASSISTANT USER LICENSE	60	07/01/2026	06/30/2036
JUSTICE PREMIER PLUS PLAN	73686	AXON EVIDENCE - STORAGE - UNLIMITED (AXON DEVICE)	60	07/01/2026	06/30/2036
JUSTICE PREMIER PLUS PLAN	73838	AXON EVIDENCE - ECOM LICENSE - PRO FOR PROSECUTOR	60	07/01/2026	06/30/2036
JUSTICE PREMIER PLUS PLAN	85762	AXON AUTO-TRANSCRIBE - JUSTICE ACCESS	60	07/01/2026	06/30/2036
JUSTICE PREMIER PLUS PLAN	85767	AXON EVIDENCE - DISCOVERY MODULE ACCESS	60	07/01/2026	06/30/2036

Services

Bundle	Item	Description	QTY
JUSTICE PREMIER PLUS PLAN	11642	AXON INVESTIGATE - THIRD PARTY VIDEO SUPPORT	60
A la Carte	100491	AXON JUSTICE - PSO - STANDARD DEPLOYMENT	1

Shipping Locations

Location Number	Street	City	State	Zip	Country
1	1400 W Lacey Blvd	Hanford	CA	93230-5905	USA

Payment Details

Jul 2026						
Invoice Plan	Item	Description	Qty	Subtotal	Tax	Total
Year 1	S00031	JUSTICE PREMIER PLUS PLAN	60	\$94,403.96	\$0.00	\$94,403.96
Invoice Upon Fulfillment	100491	AXON JUSTICE - PSO - STANDARD DEPLOYMENT	1	\$15,000.00	\$0.00	\$15,000.00
Total				\$109,403.96	\$0.00	\$109,403.96

Jul 2027						
Invoice Plan	Item	Description	Qty	Subtotal	Tax	Total
Year 2	S00031	JUSTICE PREMIER PLUS PLAN	60	\$98,180.11	\$0.00	\$98,180.11
Total				\$98,180.11	\$0.00	\$98,180.11

Jul 2028						
Invoice Plan	Item	Description	Qty	Subtotal	Tax	Total
Year 3	S00031	JUSTICE PREMIER PLUS PLAN	60	\$102,107.32	\$0.00	\$102,107.32
Total				\$102,107.32	\$0.00	\$102,107.32

Jul 2029						
Invoice Plan	Item	Description	Qty	Subtotal	Tax	Total
Year 4	S00031	JUSTICE PREMIER PLUS PLAN	60	\$106,191.61	\$0.00	\$106,191.61
Total				\$106,191.61	\$0.00	\$106,191.61

Jul 2030						
Invoice Plan	Item	Description	Qty	Subtotal	Tax	Total
Year 5	S00031	JUSTICE PREMIER PLUS PLAN	60	\$110,439.28	\$0.00	\$110,439.28
Total				\$110,439.28	\$0.00	\$110,439.28

Jul 2031						
Invoice Plan	Item	Description	Qty	Subtotal	Tax	Total
Year 6	S00031	JUSTICE PREMIER PLUS PLAN	60	\$114,856.85	\$0.00	\$114,856.85
Total				\$114,856.85	\$0.00	\$114,856.85

Jul 2032						
Invoice Plan	Item	Description	Qty	Subtotal	Tax	Total
Year 7	S00031	JUSTICE PREMIER PLUS PLAN	60	\$119,451.12	\$0.00	\$119,451.12
Total				\$119,451.12	\$0.00	\$119,451.12

Jul 2033						
Invoice Plan	Item	Description	Qty	Subtotal	Tax	Total
Year 8	S00031	JUSTICE PREMIER PLUS PLAN	60	\$124,229.16	\$0.00	\$124,229.16
Total				\$124,229.16	\$0.00	\$124,229.16

Jul 2034						
Invoice Plan	Item	Description	Qty	Subtotal	Tax	Total
Year 9	S00031	JUSTICE PREMIER PLUS PLAN	60	\$129,198.33	\$0.00	\$129,198.33
Total				\$129,198.33	\$0.00	\$129,198.33

Jul 2035						
Invoice Plan	Item	Description	Qty	Subtotal	Tax	Total
Year 10	S00031	JUSTICE PREMIER PLUS PLAN	60	\$134,366.26	\$0.00	\$134,366.26
Total				\$134,366.26	\$0.00	\$134,366.26

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

Page 6

Q-810611-46108MK

Signature

Date Signed

3/27/2026

Page 7

Q-810611-46108MK



Exhibit C

Cloud Services Addendum

1. This Cloud Services Addendum (“Addendum”) is by and between **Axon Enterprises, Inc.** (hereinafter “Contractor”) and County of Kings, a political subdivision of the State of California (hereinafter “County”). Contractor and County agree that the following terms and conditions will apply to the services provided under the Agreement of which this Addendum is incorporated therein. The parties agree to take such action to amend this Addendum from time to time as is necessary for the parties to comply with the requirements of all applicable federal and California statutes and regulations governing confidentiality, security, and privacy.

2. Definitions. Whenever used in this Addendum, the following terms shall have the meanings assigned below. Other capitalized terms used in this Addendum are defined in the context in which they are used or as defined in accompanying contract documents.

2.1 “**Agreement**” means the document provided by the County that contains terms of service, use, and work that will take place between the parties in return for consideration.

2.2 “**Confidential Data**” means any Data that a disclosing party treats in a confidential manner or that is marked “Confidential” prior to disclosure to the other party. Confidential Data does not include information which: a) is public or becomes public through no breach of the confidentiality obligations herein; b) is disclosed by the party that has received the data (the “Receiving Party”) with the prior written approval of the other party; c) was known by the Receiving Party at the time of disclosure; d) was developed independently by the Receiving Party without use of confidential Information; e) becomes known to the Receiving Party from a source other than the disclosing party through lawful means; f) is disclosed by the disclosing party to others without confidentiality obligations; or g) is required by law to be disclosed.

2.3 “**County Data**” means Data created or caused to be created by or on behalf of the County and includes credentials issued to County by Contractor and all records relating to County’s use of Contractor Services and administration of End User accounts, including any Protected Data of County personnel that does not otherwise constitute Protected Data of an End User.

2.4 “**Cover Sheet**” means the document provided by the County that incorporates all documentation, including but not limited, to the Contractor’s

Exhibits, which comprises the complete terms of the final contract that will exist between the parties.

2.5 “**Data**” means all information, whether in oral or written (including electronic) form, created by or in any way originating with County and End Users, and all information that is the output of any computer processing, or other electronic manipulation, of any information that was created by or in any way originating with County and End Users, in the course of using and configuring the Services provided under the Agreement, and includes County Data, End User Data, and Protected Data.

2.6 “**Data Compromise**” means any actual or reasonably suspected unauthorized access to or acquisition of computerized Data that compromises the security, confidentiality, or integrity of the Data, or the ability of County to access the Data. Data Compromise also means a “Breach” as defined under relevant California or federal law for Protected Data, for example, California Civil Code section 1798.29, California Health and Safety Code section 1280.15, etc.

2.7 “**Documentation**” means, collectively: a) all materials published or otherwise made available to County by Contractor that relate to the functional, operational, and/or performance capabilities of the Services; b) all user, operator, system administration, technical, support, and other manuals, diagrams, topology, and all other materials published or otherwise made available by Contractor that describe the functional, operational, and/or performance capabilities of the Services; c) any Requests for Information and/or Requests for Proposals (or documents of similar effect) issued by County, and the responses thereto from Contractor, and any document which purports to update or revise any of the foregoing; and d) the results of any Contractor presentations or tests provided by Contractor to County.

2.8 “**Downtime**” means any period of time of any duration that the Services are not made available by Contractor to County for any reason, including scheduled maintenance or Enhancements.

2.9 “**End User**” means the individuals authorized by County to access and use the Services provided by Contractor under the Agreement, including, but not limited to, employees, authorized agents, extra help, and volunteers of County; third party consultants, auditors, and other independent contractors performing services for County; any governmental, accrediting, or regulatory bodies lawfully requesting or requiring access to any Services; customers of County provided services; and any external users collaborating with County.

2.10 “**End User Data**” means Data created by an End User and includes, but is not limited to, End User account credentials and information, and all records

sent, received, or created by or for End Users, including email content, headers, and attachments, and any Protected Data of any End User or third party contained therein or in any logs or other records of Contractor reflecting End User's use of Contractor Services.

2.11 “**Enhancements**” means any improvements, modifications, upgrades, updates, fixes, revisions, and/or expansions to the Services that Contractor may develop or acquire and incorporate into its standard version of the Services or which the Contractor has elected to make generally available to its customers.

2.12 “**Force Majeure**” means an event such as an act of God; fire, flood; storm; inclement weather; earthquake; drought; riot; war or insurrection; plant or animal infestation or disease; sudden or severe energy shortage; or other condition of emergency or disaster beyond the control of the Parties which makes performance of obligations under the Agreement impossible or extremely impracticable, such obligations shall be suspended during such time any such condition or conditions exist. If a Party's duties are suspended, that Party shall resume its obligation at the earliest practical time.

2.13 “**Project Manager**” means the individual who shall serve as each Party's point of contact with the other Party's personnel as provided in this Addendum. The initial Project Managers and their contact information are set forth in the Notices section below and may be changed by a Party at any time upon written notice to the other Party.

2.14 “**Protected Data**” means Data connected to the identity of individuals and includes but is not limited to personally-identifiable information (PII), employee records, protected health information (PHI), Criminal Justice Information (CJI), Federal Tax Information (FTI) protected under Publication 1075, Social Security Administration (SSA) information, or individual financial information that is subject to state or federal laws restricting the use and disclosure of such information, including, but not limited to, Article 1, Section 1 of the California Constitution; the California Information Practices Act (Civ. Code, §§ 1798, et seq.); the California Confidentiality of Medical Information Act (Civ. Code, §§ 56, et seq.); the federal Gramm-Leach-Bliley Act (15 U.S.C. §§ 6801-6809); and the privacy and information security aspects of the Administrative Simplification provisions of the federal Health Insurance Portability and Accountability Act (45 CFR Part 160 and Subparts A, C, and E of Part 164).

2.15 “**Services**” means Contractor's computing solutions, provided over the internet to County pursuant to the Agreement, which provide the functionality and/or produce the results described in the Documentation, including without limitation all Enhancements thereto and all interfaces.

2.16 "**Third Party**" means persons, corporations, and entities other than Contractor, County, or any of their employees, contractors, or agents.

2.17 "Unsuccessful Data Compromise" means, without limitation, pings and other broadcast attacks on Contractor's firewall, port scans, unsuccessful log-on attempts, denial of service attacks, and any combination of the above, so long as no such incident results in unauthorized access, use or disclosure of County Data.

3. Scope of Addendum

3.1 The Services included under this Addendum are as determined in the Agreement, which this Addendum is attached and incorporated by reference therein.

3.2 All Services provided by Contractor that are provided online shall be Web Content Accessibility Guidelines (WCAG) 2.1 AA compliant.

4. Rights and License in and to County and End User Data

4.1 The Parties agree that as between them, all rights including all intellectual property rights in and to Data and information provided by County or on behalf of County or created by Contractor in the performance of Services hereunder, shall remain the exclusive property of County. Contractor has a limited, nonexclusive license to use End User Data and County Data and other information solely for the purpose of performing its obligations under the Agreement. This Addendum does not give Contractor any rights, implied or otherwise, data, information, or intellectual property, except as expressly stated in the Agreement.

4.2 County retains the right to use the Services to access and retrieve County and End User Data stored on Contractor's Services infrastructure at any time at its sole discretion.

4.3 Intentionally Omitted.

5. Data Privacy

5.1 Contractor shall use County Data and End User Data only for the purpose of fulfilling its duties under the Agreement and for County's and its End User's sole benefit and will not share such Data with or disclose it to any Third Party without the prior written consent of County or as otherwise required by law. By way of illustration and not of limitation, Contractor will not use such Data for Contractor's own benefit and, in particular, will not engage in "data mining" of County or End User Data or communications, whether through automated or human

means, except as specifically and expressly required by law or authorized in writing by County.

5.2 All Data will be stored on servers located solely within the Continental United States.

5.3 Contractor will provide access to County and End User Data only to those Contractor employees, contractors and subcontractors (“Contractor Staff”) who need to access the Data to fulfill Contractor’s obligations under the Agreement. Contractor will ensure that, prior to being granted access to the Data, Contractor Staff who perform work under the Agreement have all undergone and passed criminal background screenings; have successfully completed annual instruction of a nature sufficient to enable them to effectively comply with all Data protection provisions of this Addendum and the underlying Agreement; and possess all qualifications appropriate to the nature of the employees’ duties and the sensitivity of the Data they will be handling.

6. Data Security and Integrity

6.1 All facilities used to store and process County and End User Data will implement and maintain administrative, physical, technical, and procedural safeguards and best practices at a level sufficient to secure such Data in accordance with the American Institute of CPAs (AICPA)’s Service Organization Control (SOC) reporting platform SOC 2 compliance requirements. Contractor will provide proof of a current SOC 2 Compliance certification upon request (“<https://trust.axon.com/?itemUid=7bfa66da-33ab-49de-8391-e329738a1ae9&source=title>”).

6.2 Prior to the Effective Date of the Agreement, Contractor will at its expense conduct or have conducted the following, and thereafter, Contractor will, at its expense, conduct or have conducted the following at least once per year, and immediately after any actual or reasonably suspected Data Compromise:

6.2.1 A SSAE 16/SOC 2 audit of Contractor’s security policies, procedures and controls.

6.2.2 Certification under “NIST FIPS 200 AND SP 800-53”, “ISO 27001/27002”, or other acceptable standard cloud computing services certification.

6.2.3 A vulnerability scan, performed by a qualified Third-Party scanner, of Contractor’s systems and facilities that are used in any way to deliver Services under the Agreement.

6.2.4 A formal penetration test, performed by a process and qualified personnel of Contractor's systems and facilities that are used in any way to deliver Services under the Agreement.

6.3 Contractor will provide or make available to County upon written request the summary results or other documentation resulting from the above audits, certifications, scans, and tests.

6.4 Based on the results of the above audits, certifications, scans and tests, Contractor will, within Axon's SLAs and where reasonable, promptly modify its security measures in order to meet its obligations under the Agreement, and provide County with written evidence of remediation.

6.4.1 County may request that Contractor perform additional audits and tests, the summary results of which will be provided to County within seven (7) business days of Contractor's review of such results should the results of the annual audit not meet the terms of this Addendum.

6.5 Contractor shall protect County and End User Data against deterioration or degradation of Data quality and authenticity.

6.6 Contractor will provide County with service redundancy to ensure system availability in the event of natural disaster or unanticipated system outages. Redundancy shall include the following four (4) areas:

6.6.1 Hardware Redundancy

6.6.2 Processing Redundancy

6.6.3 Geographic Redundancy

6.6.4 Network Redundancy

6.7 Without limiting the foregoing, Contractor warrants that all County Data and End User Data will be encrypted in transmission (including via web interface) and in storage at a level equivalent to or stronger than 128-bit level encryption using a FIPS 140-2 certified algorithm such as AES or TLS. It is encouraged, when available and when feasible, that 256-bit encryption is used.

6.7.1 This requirement pertains to any type of sensitive data, which includes but is not necessarily limited to Confidential Data, in motion such as website access, file transfer, and email.

6.7.2 Servers which use, store, and/or process, also known as data at rest, Confidential Data shall be encrypted using FIPS 140-2 certified algorithm 128 bit or higher, such as Advanced Encryption (AES). The encryption solution must be full disk. It is encouraged, when available and when feasible, that the encryption be at 256-bit.

6.8 Contractor shall at all times ensure security vulnerabilities (hardware, software, and firmware) are appropriately patched with ninety (90) days of Contractor release. Critical security patches released by Contractors shall be patched by the Contractor within thirty (30) days of Contractor release. Patches shall be adequately tested prior to installation. If system interruption is anticipated for patch installation, County shall be notified with a minimum of forty-eight (48) hours' notice.

6.9 Contractor shall at all times use industry-standard and up-to-date security tools, technologies, and procedures, including, but not limited to, anti-virus and anti-malware protections and intrusion detection and reporting methods.

6.10 Contractor will configure the Services to filter spam while permitting communications from Third Party Internet Protocol addresses identified by County as legitimate.

6.11 Contractor will include a schedule of patches and software releases with a written report to County regarding patch installation.

6.12 Contractor will ensure multi-factor authentication of Protected Data is available when County is required to provide such authentication for regulatory compliance.

7. Data Compromise Response

7.1 Contractor shall report, in writing, to County any Data Compromise involving County or End User Data, or circumstances that could have resulted in unauthorized access to or disclosure or use of County or End User Data, not authorized by the Agreement or in writing by County, including any reasonable belief that an unauthorized individual has accessed County or End User Data. Contractor shall make the report to County immediately upon discovery of the unauthorized disclosure, but in no event more than forty-eight (48) hours after Contractor reasonably believes there has been such unauthorized use or disclosure. Oral reports by Contractor regarding Data Compromises will be reduced to writing and supplied to County as soon as reasonably practicable, but in no event more than forty-eight (48) hours after oral report. The parties acknowledge and agree that this Section constitutes notice by Contractor to County of the ongoing existence and

occurrence or attempts of Unsuccessful Data Compromises for which no additional notice to County shall be required.

7.2 Immediately upon becoming aware of any such Data Compromise, Contractor shall fully investigate the circumstances, extent and causes of the Data Compromise, and report the results to County and continue to keep County informed on a daily basis of the progress of its investigation until the issue has been effectively resolved.

7.3 Contractor's report discussed herein shall identify: a) the nature of the unauthorized use or disclosure, b) the County or End User Data used or disclosed, c) who made the unauthorized use or received the unauthorized disclosure (if known), d) what Contractor has done or shall do to mitigate any deleterious effect of the unauthorized use or disclosure, and e) what corrective action Contractor has taken or shall take to prevent future similar unauthorized use or disclosure.

7.4 Within five (5) calendar days of the date Contractor becomes aware of any such Data Compromise, Contractor shall have completed implementation of corrective actions to remedy the Data Compromise, restore County access to the Services as directed by County, and prevent further similar unauthorized use or disclosure. In the event completion of the implementation of corrective actions is not practical, Contractor shall have initiated such implementation of corrective actions.

7.5 Contractor shall cooperate with County's investigation of and response to any such Data Compromise incident.

7.6 Except as otherwise required by law, Contractor will not provide notice of the incident directly to the persons whose Data were involved, regulatory agencies, or other entities, without prior written permission from County.

7.7 Notwithstanding any other provision of the Agreement, and in addition to any other remedies available to County under law or equity, to the extent such Data Compromise was caused directly by the negligent act or willful omission of Contractor and subject to Sections 11 and 12 of the Agreement, Contractor will promptly reimburse County in full for all costs incurred by County in any investigation, remediation or litigation resulting from any such Data Compromise, including but not limited to providing notification to Third Parties whose Data were compromised and to regulatory bodies, law enforcement agencies or other entities as required by law or contract; establishing and monitoring call center(s), and credit monitoring and/or identity restoration services to assist each person impacted by a Data Compromise in such a fashion that, in County's sole discretion, could lead to identity theft; and the payment of legal fees and expenses, audit costs, fines and

penalties, and other fees imposed by regulatory agencies, courts of law, or contracting partners as a result of the Data Compromise.

8. Data Retention and Disposal

8.1 Axon will not delete Customer Content for ninety (90) days following termination. Axon Cloud Services will not be functional during these ninety (90) days other than the ability to retrieve Customer Content. Customer will not incur additional fees if Customer downloads Customer Content from Axon Cloud Services during this time. Axon has no obligation to maintain or provide Customer Content after these ninety (90) days and will thereafter, unless legally prohibited, delete all Customer Content.

8.2 Contractor shall document data backup policies; upon request of the County, shall provide proof of data backup policies.

8.3 Intentionally Omitted.

8.4 Contractor shall document data retention policies; upon request of the County, shall provide proof of data retention policies.

8.5 Axon will not delete Customer Content for ninety (90) days following termination. Axon Cloud Services will not be functional during these ninety (90) days other than the ability to retrieve Customer Content. Customer will not incur additional fees if Customer downloads Customer Content from Axon Cloud Services during this time. Axon has no obligation to maintain or provide Customer Content after these ninety (90) days and will thereafter, unless legally prohibited, delete all Customer Content. Upon written request, Contractor will supply County a certificate indicating the records disposed of, the date disposed of, and the method of disposition used. Data destruction shall be disposed of through confidential means, such as crosscut shredding or pulverizing based on National Institute of Standards and Technology (NIST) SP 800-88.

8.6 Contractor will retain logs associated with County End User activity for the length of time communicated to the Contractor by the County in the Cover Sheet, or, if no length of time is communicated, logs shall be maintained for a minimum of three (3) years or until termination of services.

8.6.1 The systems which are provided to County by Contractor shall maintain an automated audit trail that can identify the user or system process which initiates a request for Confidential Data.

8.6.2 The audit trail shall:

8.6.2.1 Be date and time stamped;

8.6.2.2 Log both successful and failed accesses;

8.6.2.3 Be read-only; and

8.6.2.4 Be restricted to authorized users.

8.6.3 Intentionally Omitted.

8.6.4 If Confidential Data is stored in the database, logging functionality shall be enabled.

8.6.5 Audit trail data shall be archived for the length of time as communicated to Contractor by the County in the Cover Sheet, if no amount is communicated, data shall be archived for at least three (3) years from the occurrence, termination of services, or as otherwise required by federal or State law.

8.7 Contractor will immediately place a “hold” on Data destruction or disposal under its usual records retention policies of records that include County’s and End User Data, in response to an oral or written request from County indicating that those records may be relevant to litigation that County reasonably anticipates. Oral requests by County for a hold on record destruction will be reduced to writing and supplied to Contractor for its records as soon as reasonably practicable under the circumstances. County will promptly coordinate with Contractor regarding the preservation and disposition of these records. Contractor shall continue to preserve the records until further notice by County.

9. Data Transfer Upon Termination or Expiration

9.1 Upon termination or expiration of the Agreement, Contractor will provide County the ability to retrieve End User Data, or a Third Party designated by County, within ninety (90) calendar days, all as further specified in the technical specifications provided in official request to Contractor. Contractor will ensure that such migration uses, facilities, and methods that are compatible with the relevant systems of County, and that County will have access to County and End User Data during the transition, in the event that it is not possible to transfer the aforementioned data to County in a format that does not require proprietary software to access the data.

9.2 Contractor will provide County with no less than ninety (90) calendar days-notice of impending cessation of its business or that of any Contractor subcontractor and any contingency plans in the event of notice of such cessation. This includes immediate transfer of any previously escrowed assets and Data to the County or its designee.

9.3 Along with the notice described above, Contractor will provide a fully documented service description and perform and document a gap analysis by examining any differences between its Services and those to be provided by its successor.

9.4 Intentionally Omitted.

9.5 Contractor shall implement its contingency and/or exit plans and take all reasonably necessary actions to provide for an effective and efficient transition of service with minimal disruption to County. Contractor will work closely with its successor to ensure a successful transition to the new service and/or equipment, with minimal Downtime and effect on County, all such work to be coordinated and performed no less than ninety (90) calendar days in advance of the formal, final transition date.

10. Service Levels

10.1 Services levels shall be provided in the manner and to the standards referenced in the Agreement, attached hereto as **Exhibit D**.

11. Interruptions in Service; Suspension and Termination of Service; Changes to Service

11.1 Notwithstanding the Force Majeure provisions contained in the Agreement, Contractor shall be responsible for providing disaster recovery Services if Contractor experiences or suffers a disaster. Contractor shall take all necessary steps to ensure that County shall not be denied access to the Services for more than twenty-four (24) hours which are critical to the business, and no more than twenty-four (24) hours, in the event there is a disaster impacting any Contractor infrastructure necessary to provide the Services. Contractor shall maintain the capability to resume provisions of the Services from an alternative location and via an alternative telecommunications route in the event of a disaster that renders the Contractor's primary infrastructure unusable or unavailable. If Contractor fails to restore the Services within twenty-four (24) hours of the initial disruption of service, County may declare Contractor to be in default of the Agreement and County may seek alternate services, which would have otherwise been provided under the Agreement, from Third Parties. Contractor shall reimburse County for all costs

reasonably incurred by County in obtaining such alternative services, with payment to be made within thirty (30) calendar days of County's written request for such payment.

11.2 In the event of a service outage, Contractor will credit County the prorated amount of fees corresponding to the time Services were unavailable.

11.3 Contractor warrants that the minimum technical requirements for access to and operation of the Services are Firefox Version 7 (or higher), Chrome Version 65 (or higher), Microsoft Edge Version 44 (or higher). Mobile browser by Firefox and Chrome. If future Enhancements to the Services require use of newer versions of these web browsers, Contractor will provide a minimum of sixty (60) days written notice to County prior to implementing such Enhancements. Any browser plug-in's (e.g. Java, ActiveX, etc.) required by Contractor for Service functionality shall be discussed with County and mutually agreed upon. Any changes to such plug-ins resulting in changes to Service functionality shall be provided to County by written notice sixty (60) days prior to implementing Enhancements.

11.4 From time to time, it may be necessary or desirable for either the County or Contractor to propose changes in the Services provided. Such changes shall be submitted to the other Party in writing for review and acceptance. Automatic Enhancements to any software used by Contractor to provide the Services that simply improve the speed, efficiency, reliability, or availability of existing Services and do not alter or add functionality, are not considered "changes to the Services" and such Enhancements will be implemented by Contractor on a schedule no less favorable than provided by Contractor to any other customer receiving comparable levels of Services.

11.5 Contractor will provide County with thirty (30) calendar days prior notice of any times that the Services will be unavailable due to non-emergency maintenance or Enhancements. Contractor will schedule any such times that the Services will be unavailable during non-business hours preferably between the hours of 12:00AM – 4:00AM PT. In the event of unscheduled and unforeseen times that the Services will for any reason be unavailable, except as otherwise prohibited by law, Contractor will immediately notify County and cooperate with County's reasonable requests for information regarding the Services being unavailable (including causes, effect on Services, and estimated duration).

11.6 County may suspend or terminate (or direct Contractor to suspend or terminate) an End User's access to Services in accordance with County's policies. County will assume sole responsibility for any claims made by End User regarding County's suspension/termination or directive to suspend/terminate such Services.

11.7 Contractor may suspend access to Services by an End User immediately in response to an act or omission that reasonably appears to jeopardize the security or integrity of Contractor's Services or the network(s) or facilities used to provide the Services. Suspension will be to the minimum extent, and of the minimum duration, required to prevent or end the security issue. The suspension will be lifted immediately once the breach is cured. Contractor may suspend access to Services by an End User in response to a material breach by End User of any terms of use End User has agreed to in connection with receiving the Services. Contractor will immediately notify County of any suspension of End User access to Services.

11.8 Contractor may suspend access to Services by County in response to an act or omission that poses a significant threat to the security or integrity of Contractor's Services or the network(s) or facilities used to provide the Services. Contractor will provide County with at least fifteen (15) business days advance written notice of intent to suspend and justification for suspension. County will have fifteen (15) business days to review and respond to such notice, and to correct any such action or omission prior to suspension. If County's response resolves the issue to the parties' mutual satisfaction, suspension will not occur. If County is unable to resolve the issue within the stated timeframe, then suspension will be to the minimum extent, and of the minimum duration, required to prevent or end the security issue. Any such suspension will be lifted immediately once the breach is cured.

12. Technical Support

12.1 Technical support shall be provided in the manner and to the standards referenced in the Agreement.

13. Transition Assistance

13.1 Contractor will develop, provide and implement the following transition assistance ("Transition Assistance") to support County's successful and uninterrupted transition from its current solution, or other solution in this area, to Contractor's Services. Transition Assistance will be provided by Contractor as detailed within the attached Axon Cloud Services Terms of Use Appendix. Transition assistance will be provided by Contractor to County at mutually agreeable dates and times.

13.2 Intentionally Omitted.

13.3 Intentionally Omitted.

13.4 Intentionally Omitted.

13.5 County agrees (a) to have the site(s) at which the Services will be used prepared in accordance with applicable Contractor requirements prior to the effective date of the installation plan and schedule; and (b) maintain the site(s) at its own expense subsequent to completion of the installation plan and schedule. County shall provide any and all necessary utility services for use of the Services.

13.6 In connection with Contractor's Transition Assistance, County will provide information, Data, computer access and time, workspace, forms, data entry and telephone service and personnel reasonably necessary to assist Contractor, consistent with County's policies and procedures.

13.7 Intentionally Omitted.

14. Protected Data

14.1 In connection with the use of the Services provided by Contractor hereunder, County may disclose to Contractor Protected Data. Contractor agrees to protect the privacy and security of Protected Data.

14.1.1 Contractor shall implement, maintain, and use appropriate administrative, technical, and physical security measures to preserve the confidentiality, integrity, and availability of the Protected Data. Contractor shall have documented countermeasures to protect physical assets in the event of a disaster. All Protected Data stored on portable devices or media must be encrypted in accordance with the Federal Information Processing Standards (FIPS) Publication 140-2. Contractor shall ensure that such security measures are regularly reviewed and revised to address evolving threats and vulnerabilities while Contractor has responsibility for the Protected Data under the terms of this Addendum. Prior to execution of the Agreement, and periodically thereafter (no more frequently than annually) at the County's request, Contractor will provide assurance, in the form of a third-party audit report or other documentation acceptable to the County.

14.2 Contractor agrees to hold the County's Protected Data, and any information derived from such information, in strictest confidence. Contractor shall not access, use or disclose Protected Data except as permitted or required by the Agreement or as otherwise authorized in writing by County, or applicable laws. If required by a court of competent jurisdiction or an administrative body to disclose Protected Data, Contractor will notify County in writing immediately upon receiving notice of such requirement and prior to any such disclosure, to give

County an opportunity to oppose or otherwise respond to such disclosure (unless prohibited by law from doing so). Any transmission, transportation, or storage of Protected Data outside the United States is prohibited except on prior written authorization by the County.

14.3 Within ninety (90) days of the termination, cancellation, expiration or other conclusion of the Agreement, Contractor shall make available the ability to retrieve the Protected Data to County unless County requests in writing that such data be securely destroyed. This provision shall also apply to all Protected Data that is in the possession of subcontractors or agents of Contractor. Such destruction shall be accomplished by “purging” or “physical destruction,” in accordance with National Institute of Standards and Technology (NIST) Special Publication 800-88. Contractor shall, upon written request, certify in writing to County that such return or destruction has been completed.

14.4 Costs. In the event of Data Compromise caused directly by the negligent act or willful omission of Contractor, Contractor agrees to promptly reimburse all costs to the County arising from such Data Compromise pursuant to federal and/or State law, including but not limited to costs of notification of individuals, establishing and operating call center(s), credit monitoring and/or identity restoration services, time of County personnel responding to Breach, civil or criminal penalties levied against the County, attorneys fees, court costs, etc. Any Data Compromise may be grounds for immediate termination of the Agreement by the County.

15. Assistance in Litigation or Administrative Proceedings

15.1 Contractor shall make itself and any employees, subcontractors, or agents assisting Contractor in the performance of its obligations under the Agreement reasonably available to County at no cost to County to testify as witnesses, or otherwise, in the event of an unauthorized disclosure caused by Contractor’s negligent act or willful omission that results in litigation or administrative proceedings against County, its directors, officers, agents, or employees based upon a claimed violation of laws relating to security and privacy and arising out of this Addendum.

16. Survival

16.1 The terms and conditions set forth in this Addendum shall survive termination of the Agreement between the Parties. If Contractor is unable to return or destroy the County’s Protected Data in accordance with the Agreement, then this Addendum, in its entirety, shall survive the Agreement until such time as Contractor does return or destroy the Protected Data.

17. Subcontractor

17.1 Contractor agrees to include substantially similar terms and conditions contained in this Addendum in all subcontractor or agency contracts providing Services under the Agreement.

Exhibit D

Service Level Agreement

Axon Cloud Services Service Level Agreement

Last Updated: September 11th, 2019

This Service Level Agreement (**SLA**) is a policy governing the use of Axon's Service Offerings (**Service Offerings**) under the terms of the Master Service Purchasing Agreement (**MSPA**) between Axon Enterprise (**Axon, us or we**) and users of Service Offerings (**you**). This SLA applies separately to each agency account using the Service Offerings. Unless otherwise provided in this SLA, this SLA is subject to the terms of the MSPA and capitalized terms have the meaning specified in the MSPA. We reserve the right to change the terms of this SLA in accordance with the MSPA. **By using Axon Cloud Services you agree that you have read and understand this SLA and you accept and agree to be bound by the following terms and conditions.** We may occasionally update 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 notify you by directly sending you a notification. In the event of a conflict between the terms of any agreement(s) between you and Axon and this SLA, the terms of those agreement(s) will control.

Definitions

- **"Downtime"** are 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 in Exclusions
- **"Incident"** a period of time in which you experience Downtime
- **"Maximum Available Minutes"** is the total accumulated minutes during a Service Month for the Service Offering
- **"Monthly Uptime Percentage"** is $(\text{Maximum Available Minutes} - \text{Downtime}) / \text{Maximum Available Minutes} * 100$
- **"Scheduled Downtime"** are periods of time, measured in minutes, in which the Service Offering is unavailable to you and in which the period of time falls within scheduled routine maintenance or planned maintenance timeframes
- **"Service Month"** is a calendar month at Coordinated Universal Time (UTC)
- **"Unavailable"** and **"Unavailability"** is when 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

We will use commercially reasonable efforts to make the Service Offerings available 99.99% of the time.

Guaranteed Service Level & Credits

If we fail to make the Service Offering available to the defined Monthly Uptime Percentage availability levels, you may be entitled to Service Credits. Service Credits are awarded as days

of Service Offering usage added to the end of the Service Offerings subscription term at no charge to you.

MONTHLY UPTIME PERCENTAGE	SERVICE CREDIT IN DAYS
Less than 99.9%	3
Less than 99.0%	7

Requesting Service Credits

In order for us to consider a claim for Service Credits, you must submit the claim to [Axon Customer Support](#) 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 our prevailing [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 us. Emergency maintenance falling outside Scheduled Routine or Planned maintenance is eligible for Service Credits

Terms

We 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 (45) 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

The Service Level Agreement does not apply to any unavailability, suspension or termination of the Service Offerings, or any other Evidence.com performance issues: (a) caused by factors outside of our reasonable control, including any force majeure event, terrorism, sabotage, virus attacks, or Internet access or 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 any 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 MSPA.

CHANGE DATE

Updated to Axon Cloud Services language

September 11th, 2019

Initial Publication

July 6th, 2016

Exhibit E

Axon Appendices

Axon Cloud Services Terms of Use Appendix

1. Definitions.

- 1.1. **"Data Controller"** means the natural or legal person, public authority, or any other body which alone or jointly with others determines the purposes and means of the processing of Personal Data.
- 1.2. **"Data Processor"** means a natural or legal person, public authority or any other body which processes Personal Data on behalf of the Data Controller.
- 1.3. **"Customer Content"** is data uploaded into, ingested by, or created in Axon Cloud Services within Customer's tenant, including media or multimedia uploaded into Axon Cloud Services by Customer. Customer Content includes Evidence but excludes Non-Content Data.
- 1.4. **"Evidence"** is media or multimedia uploaded into Axon Evidence as 'evidence' by Customer. Evidence is a subset of Customer Content.
- 1.5. **"End User"** means the natural person subject to Customer's authorized license grant who ultimately uses the Cloud Services as provided under this Agreement. End Users must adhere to the terms of use and are subject to any usage restrictions or limitations specified in this Agreement.
- 1.6. **"Non-Content Data"** is data, configuration, and usage information about Customer's Axon Cloud Services tenant, Axon Devices and client software, and users that is transmitted or generated when using Axon Devices. Non-Content Data includes data about users captured during account management and customer support activities. Non-Content Data does not include Customer Content.
- 1.7. **"Personal Data"** means any information relating to an identified or identifiable natural person. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
- 1.8. **"Provided Data"** means de-identified, de-personalized, data derived from Customer's TASER energy weapon deployment reports, related TASER energy weapon logs, body-worn camera footage, and incident reports.
- 1.9. **"Subprocessor"** means any third party engaged by the Data Processor to assist in data processing activities that the Data Processor is carrying out on behalf of the Data Controller.
- 1.10. **"Transformed Data"** means the Provided Data used for the purpose of quantitative evaluation of the performance and effectiveness of TASER energy weapons in the field across a variety of circumstances.

2. **Access.** Upon Axon granting Customer a subscription to Axon Cloud Services, Customer may access and use Axon Cloud Services to store and manage Customer Content. Customer may not exceed the total number of End Users specified in the Quote. Axon Air requires an Axon Evidence subscription for each drone operator. For Axon Evidence access granted solely for TASER, Customer may access and use Axon Evidence only to store and manage TASER CEW data ("TASER Data") and Customer may not upload non-TASER Data to Axon Evidence.

3. **Customer Owns Customer Content.** Customer controls and owns all rights, title, and interest in Customer Content. Except as outlined herein, Axon obtains no interest in Customer Content, and Customer Content is not Axon's business records. Customer is solely responsible for uploading, sharing, managing, and deleting Customer Content. Axon will only have access to Customer Content for the

limited purposes set forth herein. Customer agrees to allow Axon access to Customer Content to (a) perform troubleshooting, maintenance, or diagnostic screenings; and (b) enforce this Agreement or policies governing use of the Axon products.

4. **Security.** Axon will implement commercially reasonable and appropriate measures to secure Customer Content against accidental or unlawful loss, access or disclosure. Axon will maintain a comprehensive information security program to protect Axon Cloud Services and Customer Content including logical, physical access, vulnerability, risk, and configuration management; incident monitoring and response; encryption of uploaded digital evidence; security education; and data protection. Axon agrees to the Federal Bureau of Investigation Criminal Justice Information Services Security Addendum for its digital evidence or records management systems.
5. **Customer Responsibilities.** Customer is responsible for (a) ensuring Customer owns Customer Content or has the necessary rights to use Customer Content (b) ensuring no Customer Content or Customer End User's use of Customer Content or Axon Cloud Services violates this Agreement or applicable laws; (c) maintaining necessary computer equipment and Internet connections for use of Axon Cloud Services and (d) verify the accuracy of any auto generated or AI-generated reports. If Customer becomes aware of any violation of this Agreement by an End User, Customer will immediately terminate that End User's access to Axon Cloud Services.
 - 5.1. Customer will also maintain the security of End User usernames and passwords and security and access by end users to Customer Content. Customer is responsible for ensuring the configuration and utilization of Axon Cloud Services meet applicable Customer regulation and standards. Customer may not sell, transfer, or sublicense access to any other entity or person. If Customer provides access to unauthorized third-parties, Axon may assess additional fees along with suspending Customer's access. Customer shall contact Axon immediately if an unauthorized party may be using Customer's account or Customer Content, or if account information is lost or stolen.
 - 5.2. To the extent Customer uses the Axon Cloud Services to interact with YouTube®, such use may be governed by the YouTube Terms of Service, available at <https://www.youtube.com/static?template=terms>.
6. **Privacy.** Customer's use of Axon Cloud Services is subject to the Axon Cloud Services Privacy Policy, a current version of which is available at <https://www.axon.com/legal/cloud-services-privacy-policy>. Customer agrees to allow Axon access to Non-Content Data from Customer to (a) perform troubleshooting, maintenance, or diagnostic screenings; (b) provide, develop, improve, and support current and future Axon products and related services; and (c) enforce this Agreement or policies governing the use of Axon products.
7. **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.
8. **Storage.** For Axon Unlimited Device Storage subscriptions, Customer may store unlimited data in Customer's Axon Evidence account only if the Axon Device data is shared to Customer through Axon Evidence from a partner agency using Axon Evidence, or the data originates from Axon Capture or an Axon Device. Axon may charge Customer additional fees for exceeding purchased storage amounts. Axon may place Customer Content that Customer has not viewed or accessed for six (6) months into archival storage. Customer Content in archival storage will not have immediate availability and may take up to twenty-four (24) hours to access.
 - 8.1. **Third-Party Unlimited Storage.** For Third-Party Unlimited Storage the following restrictions apply: (i) it may only be used in conjunction with a valid Axon Evidence user license; (ii) is limited to data of the law enforcement Customer that purchased the Third-Party Unlimited Storage and the Axon Evidence End User; (iii) Customer is prohibited from storing data for other customers or law enforcement agencies; and (iv) Customer may only upload and store data that is directly related to (1) the investigation of, or the prosecution or defense of a crime, (2) common law enforcement activities, or (3) any Customer Content created by Axon Devices or Axon Evidence.
 - 8.2. **Location of Storage.** Axon may transfer Customer Content to third-party subcontractors for storage. Axon will determine the locations of data centers for storage of Customer Content If

Customer is located in the United States, Canada, or Australia, Axon will ensure all Customer Content stored in Axon Cloud Services remains in the country where Customer is located. Ownership of Customer Content remains with Customer.

9. **Suspension.** Axon may temporarily suspend Customer's or any End User's right to access or use any portion or all of Axon Cloud Services immediately upon notice, if Customer or End User's use of or registration for Axon Cloud Services may (a) pose a security risk to Axon Cloud Services or any third-party; (b) adversely impact Axon Cloud Services, the systems, or content of any other customer; (c) subject Axon, Axon's affiliates, or any third-party to liability; or (d) be fraudulent. Customer remains responsible for all fees incurred through suspension. Axon will not delete Customer Content because of suspension, except as specified in this Agreement.
10. **Axon Cloud Services Warranty.** Axon disclaims any warranties or responsibility for data corruption or errors before Customer uploads data to Axon Cloud Services. Service Offerings will be subject to the Axon Cloud Services Service Level Agreement, a current version of which is available at <https://www.axon.com/products/axon-evidence/sla>.
11. **Roles of the Parties.** To the extent that Customer is the Data Controller of Personal Data, Axon is its Data Processor. To the extent that Customer is a Data Processor of Personal Data, Axon is its Subprocessor. Notwithstanding the foregoing, to the extent any usage data (including query logs and metadata) and/or operations data (including billing and support data) in connection with Customer's use of the Services (collectively "Usage and Operations Data") is considered Personal Data, Axon is an independent Data Controller and shall Process such data in accordance with the Agreement and applicable data protection laws to develop, improve, support, and operate its products and services. For the avoidance of doubt, Axon will not disclose any Usage and Operations Data that includes confidential information with a third party except (a) in accordance with the relevant confidentiality provisions in the Agreement, or (b) to the extent the Usage and Operations Data is, in accordance with applicable data protection laws, anonymized, de-identified, and/or aggregated such that it can no longer directly or indirectly identify Customer or any particular individual.
12. **Intentionally Omitted.**
13. **Axon Records.** The following terms apply to Axon Records. Customers may purchase Axon Records either as part of an OSP 7 or OSP 10 plan or individually through a Quote.
 - 13.1. Axon Record subscription begins on the later of the (1) start date of the Quote, or (2) the date Axon provisions Axon Records to Customer. 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 plan, upon completion of the OSP 7 or OSP 10 Term ("Axon Records Subscription Term").
 - 13.2. 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. During the Customer's Axon Records Subscription Term Axon will provide Update and Upgrade releases to the Customer on an if-and-when available basis.
 - 13.3. New or additional Axon products and applications, as well as any Axon professional services needed to configure Axon Records, are not included as part of the Axon Records Subscription.
 - 13.4. End Users of Axon Records 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.
14. **Intentionally Omitted.**
15. **Intentionally Omitted.**
16. **Intentionally Omitted.**
17. **Axon Community Request Storage.** If Community Request is included as part of Customer's Quote or combined offering, 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.

18. **Performance Auto-Tagging Data.** If Axon Performance is included in Customer's Quote or a combined offering, Axon will store call for service data from Customer's CAD or RMS in order to provide services and features of Axon Performance to Customer.
19. **Axon Cloud Services Restrictions.** Customer and Customer End Users (including employees, contractors, agents, officers, volunteers, and directors), may not, or may not attempt to:
 - 19.1. copy, modify, tamper with, repair, or create derivative works of any part of Axon Cloud Services;
 - 19.2. 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;
 - 19.3. access or use Axon Cloud Services with the intent to gain unauthorized access, avoid incurring fees or exceeding usage limits or quotas;
 - 19.4. use trade secret information contained in Axon Cloud Services, except as expressly permitted in this Agreement;
 - 19.5. access Axon Cloud Services to build a competitive device or service or copy any features, functions, or graphics of Axon Cloud Services;
 - 19.6. 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
 - 19.7. use Axon Cloud Services to store or transmit infringing, libelous, or other unlawful or tortious material; material in violation of third-party privacy rights; or malicious code.
20. **After Termination.** Axon will not delete Customer Content for ninety (90) days following termination. Axon Cloud Services will not be functional during these ninety (90) days other than the ability to retrieve Customer Content. Customer will not incur additional fees if Customer downloads Customer Content from Axon Cloud Services during this time. Axon has no obligation to maintain or provide Customer Content after these ninety (90) days and will thereafter, unless legally prohibited, delete all Customer Content. Upon request, Axon will provide written proof that Axon successfully deleted and fully removed all Customer Content from Axon Cloud Services.
21. **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.
22. **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.
23. **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 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. **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.

3. **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.

4. **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:

- 4.1. **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).
- 4.2. **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.
- 4.3. **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.

5. Axon Responsibilities.

- 5.1. **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.
- 5.2. **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.
- 5.3. **Transparency.** Axon will provide documentation describing AI functionalities and their intended use and disclose any material limitations, risks, or Model Drift incidents.
- 5.4. **Incident Response.** Axon will promptly address and rectify anomalies in AI functionalities, as outlined in its incident management procedures.

- 5.5. **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.
6. **Customer Responsibilities.**
 - 6.1. **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.
 - 6.2. **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; (e) actively opt-in for programs involving data sharing through Axon's ACEIP program; and (f) provide timely feedback on Axon AI Technology performance.
 - 6.3. **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. Axon translation products may not be used by healthcare providers (doctors, nurses, paramedics, etc.) for the purpose of providing healthcare services and are only meant to allow healthcare providers to de-escalate confrontations.
7. **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:
 - 7.1. **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.
 - 7.2. **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.
 - 7.3. **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.
8. **Intentionally Omitted.**
9. **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.
10. **Auto-Transcribe.** This section outlines licensing terms for Customer's subscription of Auto-Transcribe:
 - 10.1. **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.
 - 10.2. **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.

11. Intentionally Omitted.

Axon Application Programming Interface Appendix

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

1. **Definitions.**

- 1.1. "**API Client**" means the software that acts as the interface between Customer's computer and the server, which is already developed or to be developed by Customer.
- 1.2. "**API Interface**" means software implemented by Customer to configure Customer's independent API Client Software to operate in conjunction with the API Service for Customer's authorized Use.
- 1.3. "**Axon Evidence Partner API, API or Axon API**" (collectively "**API Service**") means Axon's API which provides a programmatic means to access data in Customer's Axon Evidence account or integrate Customer's Axon Evidence account with other systems.
- 1.4. "**Use**" means any operation on Customer's data enabled by the supported API functionality.

2. **Purpose and License.**

- 2.1. Customer may use API Service and data made available through API Service, in connection with an API Client developed by Customer. Axon may monitor Customer's use of API Service to ensure quality, improve Axon devices and services, and verify compliance with this Agreement. Customer agrees to not interfere with such monitoring or obscure from Axon Customer's use of API Service. Customer will not use API Service for commercial use.
- 2.2. Axon grants Customer a non-exclusive, non-transferable, non-sublicensable, worldwide, revocable right and license during the Term to use API Service, solely for Customer's Use in connection with Customer's API Client.
- 2.3. Axon reserves the right to set limitations on Customer's use of the API Service, such as a quota on operations, to ensure stability and availability of Axon's API. Axon will use reasonable efforts to accommodate use beyond the designated limits.

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

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

- 4.1. use API Service in any way other than as expressly permitted under this Agreement;
- 4.2. use in any way that results in, or could result in, any security breach to Axon;
- 4.3. perform an action with the intent of introducing any virus, worm, defect, Trojan horse, malware, or any item of a destructive nature to Axon Devices and Services;
- 4.4. interfere with, modify, disrupt or disable features or functionality of API Service or the servers or networks providing API Service;
- 4.5. reverse engineer, decompile, disassemble, or translate or attempt to extract the source code from API Service or any related software;
- 4.6. create an API Interface that functions substantially the same as API Service and offer it for use by third parties;
- 4.7. provide use of API Service on a service bureau, rental or managed services basis or permit other individuals or entities to create links to API Service;
- 4.8. frame or mirror API Service on any other server, or wireless or Internet-based device;
- 4.9. make available to a third-party, any token, key, password or other login credentials to API Service;
- 4.10. take any action or inaction resulting in illegal, unauthorized or improper purposes; or
- 4.11. disclose Axon's API manual.

5. **API Content.** All content related to API Service, other than Customer Content or Customer's API Client content, is considered Axon's API Content, including:
 - 5.1. the design, structure and naming of API Service fields in all responses and requests;
 - 5.2. the resources available within API Service for which Customer takes actions on, such as evidence, cases, users, or reports;
 - 5.3. the structure of and relationship of API Service resources; and
 - 5.4. the design of API Service, in any part or as a whole.
6. **Prohibitions on API Content.** Neither Customer nor its End Users will use API content returned from the API Interface to:
 - 6.1. scrape, build databases, or otherwise create permanent copies of such content, or keep cached copies longer than permitted by the cache header;
 - 6.2. copy, translate, modify, create a derivative work of, sell, lease, lend, convey, distribute, publicly display, or sublicense to any third-party;
 - 6.3. misrepresent the source or ownership; or
 - 6.4. remove, alter, or obscure any confidentiality or proprietary rights notices (including copyright and trademark notices).
7. **API Updates.** Axon may update or modify the API Service from time to time ("**API Update**"). Customer is required to implement and use the most current version of API Service and to make any applicable changes to Customer's API Client required as a result of such API Update. API Updates may adversely affect how Customer's API Client access or communicate with API Service or the API Interface. Each API Client must contain means for Customer to update API Client to the most current version of API Service. Axon will provide support for one (1) year following the release of an API Update for all depreciated API Service versions.