

**SERVICE AGREEMENT**

This Service Agreement (“Agreement”) is dated December 3, 2024 (“Effective Date”) and is between the ACT 1 Group, Inc., dba ATIMS, a California corporation (“Contractor”), and the County of Fresno, a political subdivision of the State of California (“County”).

**Recitals**

A. WHEREAS, the County’s existing Jail Management System (“OffenderTrak”) has been determined to be at the end of its useful life; and

B. WHEREAS, the County has an ongoing need for the Sheriff-Coroner’s Office (FSO) to manage its day-to-day operations of its custodial facilities (the “Jail”) including incarcerated person intake, movement tracking and release, reporting, including incident reports, rule violation, and summaries, and financial accounting, including secured monies on intake, commissary expenditures, and monies added to incarcerated person’s account, and other operational requirements; and

C. WHEREAS, on March 2, 2023, the County, through its Purchasing Department, executed a request for demonstration (24-003) to competent vendors for a comprehensive Jail Management System (“JMS”), and after a detailed evaluation process on August 21, 2023, made a tentative award notice to Contractor; and

D. WHEREAS, the County now desires to enter into this Agreement with Contractor to provide software and services for the County, through its FSO, to manage its daily jail operations in accordance with the requirements set forth in this Agreement.

The parties therefore agree as follows:

**Article 1**

**Contractor’s Services**

1.1 **Scope of Services.** Contractor shall perform all of the services provided in Exhibit A to this Agreement, titled “Statement of Work”.

1 1.2 **Representation.** The Contractor represents that it is qualified, ready, willing, and  
2 able to perform all of the services provided in this Agreement.

3 1.3 **Compliance with Laws.** The Contractor shall, at its own cost, comply with all  
4 applicable federal, state, and local laws and regulations in the performance of its obligations  
5 under this Agreement, including but not limited to workers compensation, labor, and  
6 confidentiality laws and regulations.

7 1.4 **Compliance with FSO Technology Requirements.** The Contractor shall comply  
8 with technology standards and security requirements set forth in Exhibit F, entitled "Technology  
9 Standards", attached and incorporated by this reference.

10 1.5 **FBI CJIS/CA DOJ Compliance**

11 (A) Contractor represents that its ATIMS software and services store direct Criminal  
12 Justice Information (CJI) or Personally Identifiable Information ("PII"), therefore the system is  
13 required to protect all FSO data, restricted based on a need to know and right to access basis,  
14 in accordance with CJIS Security Policy guidelines.

15 (B) Contractor shall sign and submit the appropriate CA DOJ CLETS (California Law  
16 Enforcement Telecommunications System) forms (provided by FSO) to FSO CLETS  
17 Coordinator ("ACC") to keep on file for systems which may store CJI or PII from CLETS.

18 (C) Contractor's staff shall take Security Awareness Training according to the CA DOJ  
19 required interval. Contractor's staff shall register all staff within CJISOnline.com for tracking  
20 their Security Awareness Training status.

21 1.6 **Background Checks**

22 (A) Contractor's staff assigned to this Agreement shall pass the FSO standard  
23 background check (including fingerprints under FSO ORI) before entry into FSO facilities for  
24 installation or services. Contractor is solely responsible for providing adequate staffing that  
25 meets this requirement.

26 (B) Contractor's staff who are onsite or assisting remotely are required to be escorted by  
27 an FSO staff member unless they have passed a standard background check (including  
28

1 fingerprints under FSO ORI). Some FSO facilities may require an escort even if a background  
2 check has been passed, as determined by FSO.

3 (C) Contractor's staff who have access to unencrypted FSO data, or encryption keys -  
4 which allow access to encrypted Sheriff data stored in cloud services or on-premises, which  
5 may contain Criminal Justice Information (CJI) or Personally Identifiable Information (PII) shall  
6 pass the FSO standard background check (including fingerprints under FSO ORI) before  
7 accessing any FSO data stored within ATIMS systems or services.

8 (D) The Contractor shall be responsible for all costs of the FSO background check,  
9 including, but not limited to, processing fees, fingerprinting, transportation, lodging, and food.

#### 10 1.7 **Security and Privacy**

11 (A) The Contractor shall comply with technology security requirements referenced in  
12 Exhibit E.

### 14 **Article 2**

#### 15 **County's Responsibilities**

16 2.1 The County shall provide a project manager as a liaison to the Contractor who will  
17 coordinate activities with Contractor. The project manager (or designated alternate) may make  
18 decisions on behalf of the County which shall include, but not be limited to, the initiation of any  
19 change orders and the approval or acceptance of deliverables specified under this agreement.

20 2.2 The County agrees that the Contractor will retain all rights, title and interest in and to  
21 the Intellectual Property Rights of the System.

### 23 **Article 3**

#### 24 **Compensation, Invoices, and Payments**

25 3.1 The County agrees to pay, and the Contractor agrees to receive, compensation for  
26 the performance of its services under this Agreement as described in Exhibit B to this  
27 Agreement, titled "Compensation", attached and incorporated by this reference, with years one  
28 and two being \$2,676,032 - paid based on milestones and deliverables as described in Exhibit

1 B, Section I starting at "Implementation Milestone Payment Plan for First Two Years of  
2 Contract"; year three under implementation warranty with no net County cost; year four  
3 \$376,030; year five \$383,551; year six \$391,222; year seven \$399,046; year eight \$407,027;  
4 year nine \$415,168; and year ten \$423,471.

5       **3.2 Maximum Compensation.** The maximum compensation payable to the Contractor  
6 under this Agreement is Five Million, Four Hundred Seventy-one Thousand, Five Hundred  
7 Forty-Seven Dollars (\$5,471,547) for the entire ten (10) year term of this Agreement pursuant to  
8 Exhibit B - Compensation. The Contractor acknowledges that the County is a local government  
9 entity and does so with notice that the County's powers are limited by the California Constitution  
10 and by State law, and with notice that the Contractor may receive compensation under this  
11 Agreement only for services performed according to the terms of this Agreement and while this  
12 Agreement is in effect, and subject to the maximum amount payable under this section. The  
13 Contractor further acknowledges that County employees have no authority to pay the Contractor  
14 except as expressly provided in this Agreement.

15       **3.3 Invoices.** The Contractor shall submit invoices to  
16               County of Fresno, Sheriff-Coroner-Public Administrator's Office  
17               2200 Fresno Street  
18               Fresno, CA 93721-1703  
19               Attention: Account Payables

20               The Contractor shall submit each invoice within 60 days after the month in which the  
21 Contractor performs services and in any case within 60 days after the end of the term or  
22 termination of this Agreement.

23       **3.4 Payment.** The County shall pay each correctly completed and timely submitted  
24 invoice within 45 days after receipt. The County shall remit any payment to the Contractor's  
25 address specified in the invoice.

26       **3.5 Incidental Expenses.** The Contractor is solely responsible for all of its costs and  
27 expenses that are not specified as payable by the County under this Agreement.  
28

1 **Article 4**

2 **Term of Agreement**

3 4.1 **Term.** This Agreement shall become effective on the Effective Date and shall  
4 terminate eight (8) years thereafter except as provided in section 4.2, "Extension," or Article 6,  
5 "Termination and Suspension," below.

6 4.2 **Extension.** The term of this Agreement may be extended for no more than two, one-  
7 year periods only upon written approval of both parties at least 30 days before the first day of  
8 the next one-year extension period. The FSO Information Technology Division Manager or his  
9 or her designee is authorized to sign the written approval on behalf of the County based on the  
10 Contractor's satisfactory performance. The extension of this Agreement by the County is not a  
11 waiver or compromise of any default or breach of this Agreement by the Contractor existing at  
12 the time of the extension whether or not known to the County.

13 **Article 5**

14 **Notices**

15 5.1 **Contact Information.** The persons and their addresses having authority to give and  
16 receive notices provided for or permitted under this Agreement include the following:

17 **For the County:**

18 Sheriff-Coroner-Public Administrator's Office, IT Division  
19 County of Fresno  
20 2200 Fresno Street  
21 Fresno, CA 93721-1703  
22 Sheriff.Payables@fresnosheriff.org  
23 Phone: (559) 600-8100

24 **For the Contractor:**

25 The Act 1 Group, Inc., dba ATIMS  
26 Felix Rabinovich, Vice President  
27 1999 W 190<sup>th</sup> St.  
28 Torrance, CA 90504  
FelixR@atims.com

5.2 **Change of Contact Information.** Either party may change the information in section  
5.1 by giving notice as provided in section 5.3.

5.3 **Method of Delivery.** Each notice between the County and the Contractor provided  
for or permitted under this Agreement must be in writing, state that it is a notice provided under

1 this Agreement, and be delivered either by personal service, by first-class United States mail, by  
2 an overnight commercial courier service, by telephonic facsimile transmission, or by Portable  
3 Document Format (PDF) document attached to an email.

4 (A) A notice delivered by personal service is effective upon service to the recipient.

5 (B) A notice delivered by first-class United States mail is effective three County  
6 business days after deposit in the United States mail, postage prepaid, addressed to the  
7 recipient.

8 (C) A notice delivered by an overnight commercial courier service is effective one  
9 County business day after deposit with the overnight commercial courier service,  
10 delivery fees prepaid, with delivery instructions given for next day delivery, addressed to  
11 the recipient.

12 (D) A notice delivered by telephonic facsimile transmission or by PDF document  
13 attached to an email is effective when transmission to the recipient is completed (but, if  
14 such transmission is completed outside of County business hours, then such delivery is  
15 deemed to be effective at the next beginning of a County business day), provided that  
16 the sender maintains a machine record of the completed transmission.

17 **5.4 Claims Presentation.** For all claims arising from or related to this Agreement,  
18 nothing in this Agreement establishes, waives, or modifies any claims presentation  
19 requirements or procedures provided by law, including the Government Claims Act (Division 3.6  
20 of Title 1 of the Government Code, beginning with section 810).

## 21 **Article 6**

### 22 **Termination and Suspension**

23 **6.1 Termination for Non-Allocation of Funds.** The terms of this Agreement are  
24 contingent on the approval of funds by the appropriating government agency. If sufficient funds  
25 are not allocated, then the County, upon at least 30 days' advance written notice to the  
26 Contractor, may:

27 (A) Modify the services provided by the Contractor under this Agreement; or

28 (B) Terminate this Agreement.

1       **6.2 Termination for Breach.**

2           (A) Upon determining that a breach (as defined in paragraph (C) below) has  
3           occurred, the County may give written notice of the breach to the Contractor. The written  
4           notice may suspend performance under this Agreement and must provide at least 30  
5           days for the Contractor to cure the breach.

6           (B) If the Contractor fails to cure the breach to the County's satisfaction within the  
7           time stated in the written notice, the County may terminate this Agreement immediately.

8           (C) For purposes of this section, a breach occurs when, in the determination of the  
9           County, the Contractor has:

- 10           (1) Obtained or used funds illegally or improperly;  
11           (2) Failed to comply with any material part of this Agreement;  
12           (3) Submitted a substantially and knowingly incorrect or incomplete report to the  
13           County; or  
14           (4) Improperly performed any of its material obligations under this Agreement.

15       **6.3 Termination without Cause.** In circumstances other than those set forth above, the  
16       County may terminate this Agreement by giving at least 30 days advance written notice to the  
17       Contractor.

18       **6.4 No Penalty or Further Obligation.** Any termination of this Agreement by the County  
19       under this Article 6 is without penalty to or further obligation of the County.

20       **6.5 County's Rights upon Termination.** Upon termination for breach under this Article  
21       6, the County may demand repayment by the Contractor of any monies disbursed to the  
22       Contractor under this Agreement that, in the County's sole judgment, were not expended in  
23       compliance with this Agreement, including the prorated portion of the annual fee not used (e.g.,  
24       if six months are left in the term of the Agreement, one half of the annual fee). This prorated  
25       annual fee must be refunded to County thirty (30) days following notice of termination. The  
26       Contractor shall promptly refund all such monies upon demand. This section survives the  
27       termination of this Agreement.  
28

1 **Article 7**

2 **Independent Contractor**

3 7.1 **Status.** In performing under this Agreement, the Contractor, including its officers,  
4 agents, employees, and volunteers, is at all times acting and performing as an independent  
5 contractor, in an independent capacity, and not as an officer, agent, servant, employee, joint  
6 venturer, partner, or associate of the County.

7 7.2 **Verifying Performance.** The County has no right to control, supervise, or direct the  
8 manner or method of the Contractor's performance under this Agreement, but the County may  
9 verify that the Contractor is performing according to the terms of this Agreement.

10 7.3 **Benefits.** Because of its status as an independent contractor, the Contractor has no  
11 right to employment rights or benefits available to County employees. The Contractor is solely  
12 responsible for providing to its own employees all employee benefits required by law. The  
13 Contractor shall save the County harmless from all matters relating to the payment of  
14 Contractor's employees, including compliance with Social Security withholding and all related  
15 regulations.

16 7.4 **Services to Others.** The parties acknowledge that, during the term of this  
17 Agreement, the Contractor may provide services to others unrelated to the County.

18 **Article 8**

19 **Indemnity and Defense**

20 8.1 **Indemnity.** The Contractor shall indemnify and hold harmless and defend the  
21 County (including its officers, agents, employees, and volunteers) against all claims, demands,  
22 injuries, damages, costs, expenses (including attorney fees and costs), fines, penalties, and  
23 liabilities of any kind to the County, the Contractor, or any third party to the extent arising from or  
24 related to the negligence, gross negligence or willful misconduct in the performance or failure to  
25 perform by the Contractor (or any of its officers, agents, subcontractors, or employees) under  
26 this Agreement. The County may conduct or participate in its own defense without affecting the  
27 Contractor's obligation to indemnify and hold harmless or defend the County.

28 8.2 **Survival.** This Article 8 survives the termination or expiration of this Agreement.



1  
2 **Article 9**

3 **Insurance**

4 9.1 The Contractor shall comply with all the insurance requirements in Exhibit D to this  
5 Agreement.

6 **Article 10**

7 **Inspections, Audits, and Public Records**

8 10.1 **Inspection of Documents.** The Contractor shall make available to the County, and  
9 the County may examine at any time during business hours and as often as the County deems  
10 necessary, all of the Contractor's records and data with respect to the matters covered by this  
11 Agreement, excluding attorney-client privileged communications and/or other information which  
12 Contractor is prohibited from disclosing under applicable law. The Contractor shall, upon  
13 request by the County, permit the County to audit and inspect all of such records and data to  
14 ensure the Contractor's compliance with the terms of this Agreement.

15 10.2 **State Audit Requirements.** If the compensation to be paid by the County under this  
16 Agreement exceeds \$10,000, the Contractor is subject to the examination and audit of the  
17 California State Auditor, as provided in Government Code section 8546.7, for a period of three  
18 years after final payment under this Agreement. This section survives the termination of this  
19 Agreement.

20 10.3 **Public Records.** The County is not limited in any manner with respect to its public  
21 disclosure of this Agreement or any record or data that the Contractor may provide to the  
22 County, excluding records or data containing Contractor's trade secrets and confidential  
23 information if such records or data are exempt from disclosure under the California Public  
24 Records Act. Without limiting the foregoing, the County's public disclosure of this Agreement or  
25 any record or data that the Contractor may provide to the County may include but is not limited  
26 to the following:  
27  
28

1 (A) The County may voluntarily, or upon request by any member of the public or  
2 governmental agency, disclose this Agreement to the public or such governmental  
3 agency.

4 (B) The County may voluntarily, or upon request by any member of the public or  
5 governmental agency, disclose to the public or such governmental agency any record or  
6 data that the Contractor may provide to the County, unless such disclosure is prohibited  
7 by court order.

8 (C) This Agreement, and any record or data that the Contractor may provide to the  
9 County, is subject to public disclosure under the Ralph M. Brown Act (California  
10 Government Code, Title 5, Division 2, Part 1, Chapter 9, beginning with section 54950).

11 (D) This Agreement, and any record or data that the Contractor may provide to the  
12 County, is subject to public disclosure as a public record under the California Public  
13 Records Act (California Government Code, Title 1, Division 10, beginning with section  
14 7920.000) ("CPRA").

15 (E) This Agreement, and any record or data that the Contractor may provide to the  
16 County, is subject to public disclosure as information concerning the conduct of the  
17 people's business of the State of California under California Constitution, Article 1,  
18 section 3, subdivision (b).

19 (F) Any marking of confidentiality or restricted access upon or otherwise made with  
20 respect to any record or data that the Contractor may provide to the County shall be  
21 disregarded and have no effect on the County's - obligation to disclose to the public or  
22 governmental agency any such record or data unless Contractor can cite applicable  
23 authority for the exception.

24 **10.4 Public Records Act Requests.** If the County receives a written or oral request  
25 under the CPRA to publicly disclose any record that is in the Contractor's possession or control,  
26 and which the County has a right, under any provision of this Agreement or applicable law, to  
27 possess or control, then the County may demand, in writing, that the Contractor deliver to the  
28 County, for purposes of public disclosure, the requested records that may be in the possession

1 or control of the Contractor. Within five business days after the County's demand, the  
2 Contractor shall (a) deliver to the County all of the requested records that are in the Contractor's  
3 possession or control, together with a written statement that the Contractor, after conducting a  
4 diligent search, has produced all requested records that are in the Contractor's possession or  
5 control, or (b) provide to the County a written statement that the Contractor, after conducting a  
6 diligent search, does not possess or control any of the requested records. The Contractor shall  
7 cooperate with the County with respect to any County demand for such records. If the  
8 Contractor wishes to assert that any specific record or data is exempt from disclosure under the  
9 CPRA or other applicable law, it must deliver the record or data to the County and assert the  
10 exemption by citation to specific legal authority within the written statement that it provides to  
11 the County under this section. The Contractor's assertion of any exemption from disclosure is  
12 not binding on the County, but the County will give at least 10 days' advance written notice to  
13 the Contractor before disclosing any record subject to the Contractor's assertion of exemption  
14 from disclosure. The Contractor shall indemnify the County for any court-ordered award of costs  
15 or attorney's fees under the CPRA that results from the Contractor's delay, claim of exemption,  
16 failure to produce any such records, or failure to cooperate with the County with respect to any  
17 County demand for any such records.

## 18 **Article 11**

### 19 **Disclosure of Self-Dealing Transactions**

20 11.1 **Applicability.** This Article 11 applies if the Contractor is operating as a corporation  
21 or changes its status to operate as a corporation.

22 11.2 **Duty to Disclose.** If any member of the Contractor's board of directors is party to a  
23 self-dealing transaction, he or she shall disclose the transaction by completing and signing a  
24 "Self-Dealing Transaction Disclosure Form" (Exhibit C to this Agreement) and submitting it to  
25 the County before commencing the transaction or immediately after.

26 11.3 **Definition.** "Self-dealing transaction" means a transaction to which the Contractor is  
27 a party and in which one or more of its directors, as an individual, has a material financial  
28 interest.

1 **Article 12**

2 **General Terms**

3 12.1 **Modification.** Except as provided in Article 6, "Termination and Suspension," this  
4 Agreement may not be modified, and no waiver is effective, except by written agreement signed  
5 by both parties. The Contractor acknowledges that County employees have no authority to  
6 modify this Agreement except as expressly provided in this Agreement.

7 12.2 **Non-Assignment.** Neither party may assign its rights or delegate its obligations  
8 under this Agreement without the prior written consent of the other party.

9 12.3 **Governing Law.** The laws of the State of California govern all matters arising from  
10 or related to this Agreement.

11 12.4 **Jurisdiction and Venue.** This Agreement is signed and performed in Fresno  
12 County, California. Contractor consents to California jurisdiction for actions arising from or  
13 related to this Agreement, and, subject to the Government Claims Act, all such actions must be  
14 brought and maintained in Fresno County.

15 12.5 **Construction.** The final form of this Agreement is the result of the parties' combined  
16 efforts. If anything in this Agreement is found by a court of competent jurisdiction to be  
17 ambiguous, that ambiguity shall not be resolved by construing the terms of this Agreement  
18 against either party.

19 12.6 **Days.** Unless otherwise specified, "days" means calendar days.

20 12.7 **Headings.** The headings and section titles in this Agreement are for convenience  
21 only and are not part of this Agreement.

22 12.8 **Severability.** If anything in this Agreement is found by a court of competent  
23 jurisdiction to be unlawful or otherwise unenforceable, the balance of this Agreement remains in  
24 effect, and the parties shall make best efforts to replace the unlawful or unenforceable part of  
25 this Agreement with lawful and enforceable terms intended to accomplish the parties' original  
26 intent.

27 12.9 **Nondiscrimination.** During the performance of this Agreement, the Contractor shall  
28 not unlawfully discriminate against any employee or applicant for employment, or recipient of

1 services, because of race, religious creed, color, national origin, ancestry, physical disability,  
2 mental disability, medical condition, genetic information, marital status, sex, gender, gender  
3 identity, gender expression, age, sexual orientation, military status or veteran status pursuant to  
4 all applicable State of California and federal statutes and regulation.

5 12.10 **No Waiver.** Payment, waiver, or discharge by the County of any liability or obligation  
6 of the Contractor under this Agreement on any one or more occasions is not a waiver of  
7 performance of any continuing or other obligation of the Contractor and does not prohibit  
8 enforcement by the County of any obligation on any other occasion.

9 12.11 **Entire Agreement.** This Agreement, including its exhibits, is the entire agreement  
10 between the Contractor and the County with respect to the subject matter of this Agreement,  
11 and it supersedes all previous negotiations, proposals, commitments, writings, advertisements,  
12 publications, and understandings of any nature unless those things are expressly included in  
13 this Agreement. If there is any inconsistency between the terms of this Agreement without its  
14 exhibits and the terms of the exhibits, then the inconsistency will be resolved by giving  
15 precedence first to the terms of this Agreement without its exhibits, and then to the terms of the  
16 exhibits.

17 12.12 **No Third-Party Beneficiaries.** This Agreement does not and is not intended to  
18 create any rights or obligations for any person or entity except for the parties.

19 12.13 **Consistent Federal Income Tax Position.** Contractor acknowledges that the Jail  
20 Facilities have been acquired, constructed, and/or improved using net proceeds of  
21 governmental tax-exempt bonds (collectively, "Bond-Financed Facilities"). Contractor agrees  
22 that, with respect to this Agreement and the Bond Financed Facilities, Contractor is not entitled  
23 to take, and shall not take, any position (also known as a "tax position") with the Internal  
24 Revenue Service ("IRS") that is inconsistent 14 with being a "service provider" to the County, as  
25 a "qualified user" with respect to the Bond Financed Facility, as "managed property," as all of  
26 those terms are used in Internal Revenue Service Revenue Procedure 2017-13, and to that  
27 end, for example, and not as a limitation, Contractor agrees that Contractor shall not, in  
28 connection with any federal income tax return that it files with the IRS or any other statement or

1 information that it provides to the IRS, (a) claim ownership, or that it is a lessee, of any portion  
2 of the Bond Financed Facilities, or (b) claim any depreciation or amortization deduction,  
3 investment tax credit, or deduction for any payment as rent with respect to the Bond-Financed  
4 Facilities.

5 **12.14 Authorized Signature.** The Contractor represents and warrants to the County that:

6 (A) The Contractor is duly authorized and empowered to sign and perform its  
7 obligations under this Agreement.

8 (B) The individual signing this Agreement on behalf of the Contractor is duly  
9 authorized to do so and his or her signature on this Agreement legally binds the  
10 Contractor to the terms of this Agreement.

11 **12.15 Electronic Signatures.** The parties agree that this Agreement may be executed by  
12 electronic signature as provided in this section.

13 (A) An "electronic signature" means any symbol or process intended by an individual  
14 signing this Agreement to represent their signature, including but not limited to (1) a  
15 digital signature; (2) a faxed version of an original handwritten signature; or (3) an  
16 electronically scanned and transmitted (for example by PDF document) version of an  
17 original handwritten signature.

18 (B) Each electronic signature affixed or attached to this Agreement (1) is deemed  
19 equivalent to a valid original handwritten signature of the person signing this Agreement  
20 for all purposes, including but not limited to evidentiary proof in any administrative or  
21 judicial proceeding, and (2) has the same force and effect as the valid original  
22 handwritten signature of that person.

23 (C) The provisions of this section satisfy the requirements of Civil Code section  
24 1633.5, subdivision (b), in the Uniform Electronic Transaction Act (Civil Code, Division 3,  
25 Part 2, Title 2.5, beginning with section 1633.1).

26 (D) Each party using a digital signature represents that it has undertaken and  
27 satisfied the requirements of Government Code section 16.5, subdivision (a),  
28

1 paragraphs (1) through (5), and agrees that each other party may rely upon that  
2 representation.

3 (E) This Agreement is not conditioned upon the parties conducting the transactions  
4 under it by electronic means and either party may sign this Agreement with an original  
5 handwritten signature.

6 12.16 **Counterparts.** This Agreement may be signed in counterparts, each of which is an  
7 original, and all of which together constitute this Agreement.

8 12.17 **Limitation of Liability.** To the maximum extent permitted by applicable law and  
9 notwithstanding any provision herein to the contrary, neither County nor Contractor shall have  
10 any liability for any indirect, consequential, special or incidental damages, damages for loss of  
11 profits or revenues, whether in an action in contract or tort, even if such party has been advised  
12 of the possibility of such damages, unless such party has engaged in gross negligence or willful  
13 misconduct or the damages arise from a claim for which a party is entitled to indemnification in  
14 this Agreement.

15 \\\

16 \\\

17 \\\

18

19

20

21

22

23

24

25

26

27

28

1 The parties are signing this Agreement on the date stated in the introductory clause.

2 The ACT 1 Group, Inc., dba ATIMS

COUNTY OF FRESNO

3  
4 



5 Felix Rabinovich, Vice President

Nathan Magsig, Chairman of the Board of Supervisors of the County of Fresno

6 1999 W 190<sup>th</sup> St.  
7 Torrance, CA 90504

**Attest:**  
Bernice E. Seidel  
Clerk of the Board of Supervisors  
County of Fresno, State of California

9  
10 By:   
Deputy

11 For accounting use only:

12 Org No.: 31112425  
13 Account No.: 7281  
14 Fund No.: 0001  
15 Subclass No.: 10000



## Table of Contents

<b>1 Statement of Work Overview</b> .....	3
<b>1.1 Objectives</b> .....	3
<b>1.2 Project Management</b> .....	3
<b>1.3 Change Control</b> .....	3
<b>2 Scope of Work</b> .....	4
<b>2.1 Deliverables</b> .....	4
<b>2.1.1 Deliverable Details</b> .....	6
<b>2.2 Period of Performance</b> .....	8
<b>2.3 Project Schedule</b> .....	8
<b>2.4 Project Management Communication</b> .....	10
<b>2.5 Issue Resolution</b> .....	10
<b>2.6 System Requirements and Design</b> .....	11
<b>3 System Interfaces</b> .....	11
<b>4 Technical Architecture</b> .....	11
<b>5 Data Conversion</b> .....	11
<b>6 Testing</b> .....	12
<b>7 Training</b> .....	13
<b>8 Acceptance Criteria</b> .....	13
<b>8.1 Project Deliverable Acceptance Criteria</b> .....	13
<b>8.2 Software Deliverable Acceptance Criteria</b> .....	13
<b>8.3 Project Issue Resolution</b> .....	14
<b>8.4 Defect Severity and Definition</b> .....	16
<b>9 System Documentation</b> .....	17
<b>10 Release Implementation</b> .....	17
<b>11 Post Release Implementation Support</b> .....	17
<b>12 Sample Required Interfaces / Exchanges</b> .....	22

## **1 Statement of Work Overview**

This Statement of Work (SOW) is by and between ATIMS and FRESNO COUNTY SHERIFF'S OFFICE (FSO). It describes the principal activities and responsibilities of ATIMS and FSO to install ATIMS Jail Management System ("JMS" or "Software") FSO's detention facilities.

FSO has decided on an on-premises solution and this SOW contains details of how the project will be executed and describes the work activities, deliverables, and timeline for the execution of this project as defined within.

This SOW may be updated as required throughout the life of the JMS implementation. The parties will mutually agree upon dates that correspond with changes to this SOW, including those for additional scope or services.

### **1.1 Objectives**

FSO expects the new JMS will deliver new and best-in-class industry standards based on operational capabilities, drive operational productivity, improve the safety of its personnel and inmates and provide a high-performing platform for the next generation of JMS users.

### **1.2 Project Management**

The ATIMS Project Management shall plan the activities to be carried out in the project, the assignment of resources to those activities, the dependencies among those activities, and their timing. The ATIMS PM Team shall establish a project control and reporting system, using a combination of MS Project and JIRA, to provide routine and realistic assessments of the project progress through the completion of the project against approved milestones and detailed plans. Working with the Agency JMS Project Manager, the ATIMS Team Project Manager shall set up roles, responsibilities, record-keeping systems, lines of communication, and procedures for managing the project, assuring quality, managing technical configuration, and controlling project changes.

The ATIMS Team Project Manager shall provide on-going project management including regular (weekly) project plan updates, weekly status reports and weekly status meetings. The ATIMS PM Team shall prepare a baseline risk management plan and update the plan regularly (monthly) over the course of the project.

### **1.3 Change Control**

The change control process is required to:

- assess and document the impact of scope changes on project schedules, resources, prices, payment schedule, deliverables, acceptance criteria, and other provisions of this SOW impacted by the proposed change;
  - provide a formal vehicle for approval to proceed with any changes to this SOW and;
  - provide a project audit record of all material changes to the original SOW.
- A. Any changes, additions or deletions to the work effort hereunder including to the scope of work, will be handled as follows:
- I. In the case where FSO or ATIMS determine a change is required or desirable to the project, the requesting party will complete a change request form (Change Request or CR) and advance the CR for sign off by the other party;
  - II. Upon execution by each party, a CR will become a Change Order and form part of this SOW; and
  - III. If the Parties do not execute and deliver to one another a Change Order, the prior obligations of each party under this SOW will remain unchanged.
- B. The Project Sponsors and Project Managers (FSO and ATIMS) must approve all changes to this SOW, pursuant to a Change Order.
- C. In a situation where a proposed change will impact the project significantly, whether it be time, money or scope, a Change Order may need to operate as a separate and unique work assignment independent of the project schedule, resources, price, payment schedule, deliverables, milestones, acceptance criteria or other provisions of this SOW.
- D. If and when required, the FSO will ensure each and every Change Order is accompanied by the appropriate pre-approved payment vehicle (purchase order, contract amendment or otherwise) to facilitate billing by ATIMS.

## 2 Scope of Work

The work/deliverables to be performed/provided by the ATIMS team, in alignment and compliance with FSO RFP Requirements, are documented below.

### 2.1 Deliverables

At a high level, the FSO JMS project scope includes:

## Exhibit A

- Project Management – ATIMS has designated [ATIMS PM] as the Project Manager who will manage the coordination and workload of ATIMS team members. ATIMS understands that [AGENCY PM] has been appointed as the Project Manager by the FSO to manage all project activities on behalf of the Agency.
- Status meetings to be held weekly; the parties will agree upon location during the initiation phase of the project.
- A Kickoff event, attended by the ATIMS Team Project Manager, one (1) ATIMS SME and one (1) ATIMS Business Analyst.
- ATIMS out-of-the-box Jail Management System functionality is baseline for the JMS implementation.
- Up to ten (10) customized electronic forms; including one pre-book arrest form, one medical pre-screening form, one classification, one re-classification and one property receipt form as identified/discussed during project discovery . Additional forms beyond the 10 may be created, at cost.
- ATIMS offers 200+ canned out-of-the-box reports expected to meet most reporting requirements, plus up to five (5) custom reports identified during project discovery assuming the standard system reports do not meet the FSO need. Additional reports may be created, at cost.
- Pre-Implementation Analysis, comprised of an in-depth review of agency processes, interviews with subject matter experts (SMEs), analysis of currently used tools (Excel) and how they are used in everyday work and the validation of all ATIMS functional modules.
- Testing and Delivery of identified Customizations.
- Migration / Conversion of data from legacy system(s) - ATIMS will work with the FSO team to analyze the needs for historical data, recommend and design a conversion approach, and migrate data into the target solution.
- Configuration Support – ATIMS will guide the FSO in configuration activities. ATIMS will use a scripting process to automate the migration of configuration preferences across multiple environments (test, training, and prod).
- Functional Requirements Definition and Design for any identified customizations.
- Training, including system admin and train-the-trainer training as well as end-user training, if required. ATIMS will prepare and execute a detailed training plan to identify the approach, methods and activities associated with all project training.
- Documentation – ATIMS will provide product documentation, release notes (where appropriate) and other materials in electronic format.

- Data Exchanges / Interfaces - ATIMS will perform interface analysis, configuration and testing for interfaces included in this project, utilizing the ATIMS interface engine.
- At least a one (1) month User Acceptance Testing (UAT) period.
- Onsite go-live support commencing immediately after UAT as per the Agreement.
- Transition – ATIMS will ensure that FSO team is prepared to manage the production environment after going live.
- Support & Maintenance – ATIMS will support and maintain the ATIMS JMS production implementation as per the Agreement. **Annual Allotment of Support Hours.** Additionally, ATIMS offers an allotment of hours each year as part of your Support & Maintenance Agreement and that allotment can be used towards training, building reports/forms/interfaces, etc.

## 2.1.1 Deliverable Details

- **Reports**
  - 200 Canned/Out-of-the-box reports. ATIMS has approximately 200 canned, out-of-the-box reports available for use by all agencies. It is anticipated that a lot of the canned reports will meet FSO's needs.
    - ATIMS will work with your staff during gapfit (done during Kickoff) and implementation to ensure these canned reports meet the majority of your needs.
    - 5 customized reports are included with implementation, that are typically identified during discovery that we will build for you.
    - If add'l customized reports needed. In the event FSO needs additional assistance customizing reports, those can be included in the implementation/build, but will be priced at cost (\$200/hr \* quoted hours/days - typically \$5,000 ea. - 3 days). Some more comprehensive reports may be more like 4-5 days, i.e. \$6,400 to \$8,000 ea. We'll provide a quote once we understand what is needed.
  - Training Plan. As part of the Training Phase of Implementation (in advance of Go Live), ATIMS will work with FSO Train-the-Trainers and Administrators to develop a Training Plan, which always includes training on how to build reports.
  - Training/Tools for Customized Reports. ATIMS will provide the training and tools necessary for FSO to develop and add additional customized reports as needed. The skills that are required for such development are general T-SQL, HTML, JavaScript and CSS skills. ATIMS has licensed the JSReports library, that includes browser-based development environment (IDE). ATIMS will teach reports developers (typically System

## Exhibit A

Administrator level personnel) how to develop custom reports and integrate them into JMS.

- **Forms**
  - ATIMS offers up to 10 electronic forms to be built for you; they are typically identified during discovery/gapfit.
    - Many times the information input into legacy hard-copy forms is already part of the JMS and do not require an actual form to be built.
    - 5 custom forms (medical prescreening, classification and reclassification, pre-book arrest and property receipt) are standard and included in the 10 forms to be built as part of implementation. These forms are ALWAYS customized to each client, and as part of the 10, are not an additional charge.
    - If additional customized forms needed. In the event FSO needs additional forms, those can be included in the implementation/build, but will be priced at cost (\$200/hr \* quoted hours/days - typically \$8,000 ea - 5 days). Forms due to their extensive capabilities require more build time and are more expensive. We'll provide a quote once we understand what is needed.
  - Training Plan. As part of the Training Phase of Implementation (in advance of Go Live), ATIMS will work with Agency Train-the-Trainers and Administrators to develop a Training Plan, which includes training on how to build forms if the Agency has staff that has the knowledge base and desire to be trained.
  - Training/Tools for Customized Forms. ATIMS will provide the training and tools necessary for FSO to develop and add additional customized forms as needed. The skills that are required for such development are general T-SQL, HTML, JavaScript and CSS skills. ATIMS will teach reports developers (typically System Administrator level personnel) how to develop custom forms and integrate them into JMS.
- **Annual Allotment of Support Hours**. Additionally, this Agreement includes an allotment of hours each year as part of your Support & Maintenance Agreement and that allotment can be used towards training, building reports/forms/interfaces, etc.
- **API Capabilities**.
  - All interfaces Listed in Exhibit A section 12 will be developed as part of implementation; with the need to modify application code.

- The ATIMS Interface engine is an encompassing solution to allow data exchange to occur without the need to custom code solutions. Real-time Messaging interface – Outbound. Interface Engine can be configured to invoke external web service (REST or legacy SOAP). The return data for GET calls can be configured to be processed by Stored procedure.
  - Real-time Messaging interface – Inbound. Interface Engine can be configured to listen for external applications to invoke web service (with authentication) and process the result using Stored Procedures or custom C# code.
  - Folder Watch – This method is configured in the administration page of ATIMS JMS. It allows the user to configure a UNC folder path to be monitored to accept data or files into ATIMS. Mapping of data uses stored procedures. This can be used to accept scanned PDF attachments, photos from 3rd party systems, data exports from 3rd party systems.

## 2.2 Period of Performance

The project work will be tracked to the duration defined in Section 2.3 below. The FSO is responsible for reporting against testing progress and overall status during UAT.

The final project schedule will be defined and approved in collaboration with the FSO PM during the initiation stage of this project. The change control process outlined in this SOW shall govern changes to the approved Project Schedule.

## 2.3 Project Schedule

A draft project schedule will be developed by ATIMS and submitted for approval/review by FSO. The project schedule will be used for planning and tracking purposes. The ATIMS Project Management Team will work with the FSO PM to maintain an updated project schedule. FSO deliverables that impact ATIMS timelines will be represented in the project schedule as milestones. The FSO can drive schedule changes using the Change Control Process.

The project schedule consists of 4 stages: Inception, Elaboration, Construction, and Transition.

The Inception Phase is dedicated to the project initiation and planning of the project and typically begins with the kickoff meeting. In the graph above we have not identified every project planning document, but it is during this stage that these documents are completed, reviewed and approved.

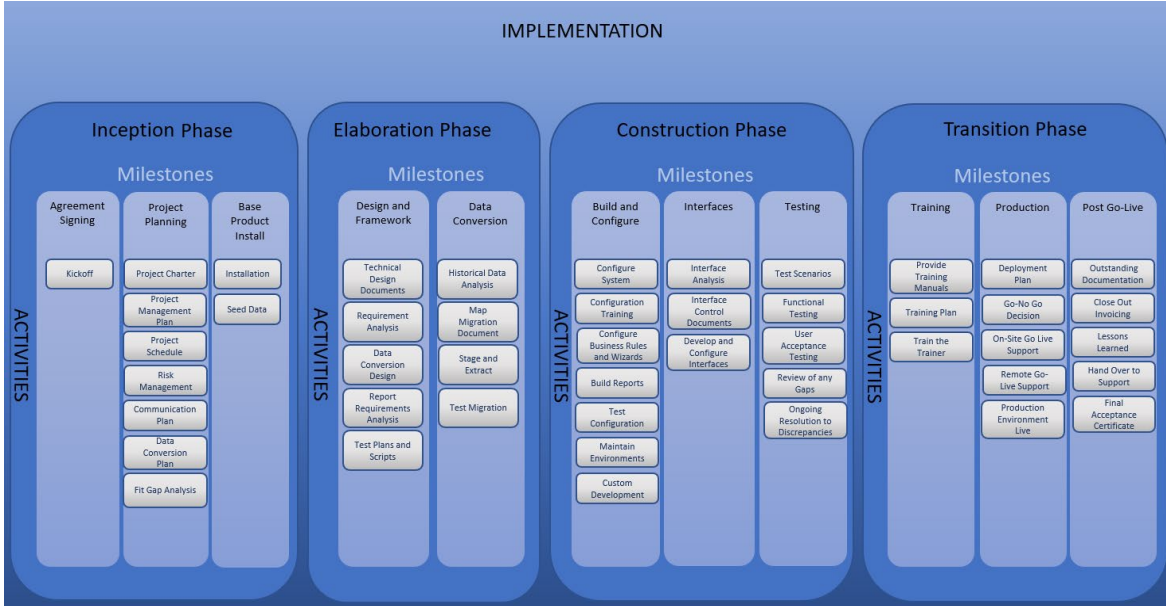
During the inception stage of the project the FSO PM and ATIMS PM will ensure that any dependencies between FSO activities (such as deliverable reviews / approvals or Organizational Change Management activities) are integrated into ATIMS' master project schedule at the relevant points (i.e., major tasks and/or milestones).

The Elaboration Phase is the time period in which ATIMS typically delivers the base installation of the product application. Requirement validation, requirement analysis and design work are also completed during this stage of the project. During this phase ATIMS will be working closely with FSO to also define the configuration for the application. As seen by the graph above the Inception Phase and the Elaboration Phase have many overlapping tasks that can be completed in a concurrent manner. With the level of concurrent activities during these first two stages, careful consideration and planning is required to ensure resources are not over allocated.

The Construction Phase is the phase of the project in which most of the development work is completed. The four main tasks in this phase will be the development of data migration, interfaces, enhancements, and forms. The testing team will test the construction of these tasks as they are made available. As the construction of these tasks is completed and tested, ATIMS shall deliver this to the FSO environment to demonstrate its adherence and validation of the RTM. For the sake of better quality and engaged stakeholders, this is done in an iterative and incremental manner. The Construction Phase is typically the longest phase of the project.

The Transition Phase is the deployment and training stage, in preparation of a go-live date. The FSO user acceptance testing will take place during this stage as well. From a planning perspective, it is usually during this phase that a solid Go-Live date is defined. It is also during this stage that the client will enter into the Post Go-Live (Maintenance) in which ATIMS Support will take over the project from the Implementation Team.





## 2.4 Project Management Communication

The project communication between the FSO and the ATIMS PM Team will consist of regular weekly status meetings to ensure all aspects of the project are discussed and remain on track. Scheduling of the status meetings, agendas, minutes and escalation will be defined and agreed to between the FSO and ATIMS project management teams during the initial preparation stage of the project. Schedules and appropriate escalation trees will be communicated to all responsible stakeholders including the JMS Steering Committee. The primary points of contact will be the project managers for ATIMS and the FSO.

## 2.5 Issue Resolution

ATIMS will maintain a project issues/risk log for all issues raised during the life cycle of the project. This issue log will be reviewed, actioned during status meetings, and reported upon on a regular basis as defined by the project management team. Additionally, ATIMS utilizes issues management software (JIRA) to track client reported issues. During testing, each tester will have their own account to log and track reported issues.

## **2.6 System Requirements and Design**

Evaluation of system requirements is conducted throughout the project lifecycle with the accompanying deliverables considered living documents intended to convey a shared understanding of how the ATIMS JMS can, will, and does meet the requirements of FSO. After definition of the expectations for each deliverable document, updates will be regularly provided to track new findings and solutions.

## **3 System Interfaces**

For purposes of this Systems Interfaces section of the Statement of Work, the term 'JMS Interfaces' shall be defined to be the set of all interfaces identified in Section 12 of this Exhibit A.

ATIMS shall provide an overview of interface capability and inventory of interfaces available with the out-of-box JMS. ATIMS shall work with the FSO to identify existing APIs or other methods for the JMS to receive or provide data for each JMS Interface.

For JMS Interfaces, ATIMS shall also provide API(s) or other method(s) for the JMS to provide data to or receive data from the Integrated Sharing Environment (i.e., expose the JMS interface to the ISE). ATIMS shall repurpose JMS APIs utilized in point-to-point interfaces for use in ISE data exchanges where practical. The FSO shall use these APIs or other methods to include data from JMS Interfaces in other data exchanges as required. The FSO shall design and implement data transformations and data transport mechanisms for such exchanges. The FSO shall provide modifications to external systems as required to support such exchanges. ATIMS shall support integration and testing of such data exchanges by the FSO.

After acceptance of the Interface Design Deliverable, the FSO may request ATIMS to provide additional interface implementation services. Authorization for such additional services will be at the FSO's sole discretion and subject to the change order process.

## **4 Technical Architecture**

ATIMS shall confirm and update technical environment specifications required to host the JMS. The FSO shall provide and install specified infrastructure, as appropriate. ATIMS shall install, configure and test the installation of all JMS components. ATIMS shall specify, install, configure and test three (3) environments (e.g., test, training, and production) as appropriate.

## **5 Data Conversion**

ATIMS shall work with the FSO to determine data to be converted and migrated from legacy FSO/FSO systems. ATIMS shall develop and test scripts to extract data from source systems,

transform data as required, and load data into JMS. The FSO will extract data from the FSO system, move it to the FSO data warehouse and do basic data cleansing. ATIMS will pick-up the data from that staging environment and proceed from there.

ATIMS shall provide exception reporting (Excel/SQL Table) for all data that fails the conversion process due to source data issues.

ATIMS shall perform at a minimum four (4) full test data conversions. After each test data conversion, ATIMS shall provide data exception reports with remediation recommendations, including adjustments to the data conversion scripts or source system data corrections. ATIMS shall modify and adjust conversion scripts as required before performing the next test data conversion.

ATIMS shall perform and confirm the final data conversion as part of User Acceptance Test and at System Cutover.

## **6 Testing**

ATIMS shall prepare test plans and conduct testing needed to ensure that all system components are complete, integrated, and error free, and meet system requirements and specifications. Progressive test cycles shall be repeated until all bugs and anomalies are resolved and the system components are demonstrated to meet all applicable criteria, specifications, and system requirements.

ATIMS shall conduct unit/module and systems integration testing as specified in the Test Plan.

ATIMS shall develop test plans and perform tests to ensure that the production system will meet all response-time requirements when deployed to all users and used during peak workloads. ATIMS shall tune and otherwise update the production system to resolve noted issues. ATIMS shall repeat stress-test cycles until all issues are resolved. ATIMS shall conduct failover and recovery testing to ensure that the high availability and business continuity goals are met by the implementation.

The FSO shall conduct User Acceptance Testing (UAT) as specified in the Test Plan. ATIMS shall support UAT with timely response and assistance to ensure reasonable adherence to the previously agreed upon schedule. ATIMS shall respond to critical and High priority issues (that could delay UAT completion) within 1 hour during designated UAT test windows, and shall resolve critical issues as soon as possible, with a 2-hour status update.

ATIMS shall prepare system environments, including configuration and loading of test data, required to support all testing as specified in the Test Plan.

ATIMS shall record all tests conducted, defects discovered, defects resolved and retests. ATIMS shall provide regular status reporting of all testing.

## **7 Training**

ATIMS shall provide full on-site training. The FSO shall employ a “Train-the-Trainer” approach following the initial training and in-between the interim refresher training schedules. ATIMS shall train a percentage of jail staff members who are qualified as “super users” (these users usually become trainers and have a greater knowledge of the entire system).

FSO shall designate a percentage of jail staff for such training. After training, such super users will be knowledgeable of all modules of the JMS and be able to resolve issues or identify problems regardless of their current position assignment. Super users will train other FSO employees under the Train-the-Trainer approach.

ATIMS shall provide training for the following roles. Training shall be specific to each listed role:

- A. System Administrator
- B. Super User – “Train the Trainer”
- C. JMS End User (by functional group), if required

## **8 Acceptance Criteria**

### **8.1 Project Deliverable Acceptance Criteria**

Following delivery of each project deliverable (non-software deliverables such as project schedule, conceptual design document, etc.) the FSO will have a period of ten (10) working days (Acceptance Review Period) to verify that each project deliverable meets expectations.

If, during the Acceptance Review Period, the FSO determines that the deliverable is deficient then ATIMS shall provide a timeline to modify or correct the deliverable. Following delivery of each modification the FSO shall have ten working (10) days to verify the modification after which period it is deemed accepted. If no issues are raised within the Acceptance Review Period, or the deliverable or any portion of the deliverable is used or relied upon in the subsequent project activities, then the deliverable is deemed accepted.

### **8.2 Software Deliverable Acceptance Criteria**

Following deployment of the software deliverable, the FSO shall have a period of at least one (1) month to conduct UAT to verify the software deliverable substantially performs in the manner of which it was originally intended by the FSO (the Acceptance Period).

If, during UAT, the FSO determines that the deliverable does not meet their needs, or identifies an obvious defect, the FSO shall notify the ATIMS Project Manager in writing, and the ATIMS PM Team

shall provide a timeline for addressing the need through the change control process or resolution of the defect. All reported, bona fide defects will be triaged and categorized in accordance with the defect severity and definition table in section 10.4. ATIMS acknowledges and agrees to use its best efforts to install all patches (in sequential order). Once patches are installed, FSO will confirm whether this resolve the reported defect(s) within five (5) days of delivery; after which period the repair is deemed accepted unless testing determines that the implemented fix does not resolve the problem, in which case the ATIMS PM Team will work to immediately resolve the issue.

If a mutually agreed Severity Level 1, Level 2 or Level 3 defect (Sec. 8.4) is identified, and such defect has a material impact on continued UAT progress so as to stop or substantially slow down the UAT process, until a resolution is provided ATIMS will extend the UAT period for that defect only, or any additional mutually agreed Severity Level 1, 2 or 3 defect, which would not have been identified through testing as a result of the initial defect blocking UAT progress.

In each case, the parties will:

- (a) assess the magnitude of the reported defect and the timeline required to provide resolution;
- (b) determine the appropriate period of time needed to re-test, including regression testing and;
- (c) determine a mutually agreeable revised project schedule that may incorporate an extension to the UAT period and, if appropriate, an extension to the project period of performance.

If no defects are reported within the Acceptance Period, or the deliverable or any portion of the deliverable is used in production, then the deliverable is deemed accepted. Any issues found after the Acceptance Period will be addressed under the annual support and maintenance services contract.

Defects are to be considered unique entities and cannot be attached to one another except for reporting purposes. Resolution to one defect may introduce new defects. Those new defects are considered unique and will be managed according to their unique presentation. Acceptance of a software deliverable cascades acceptance to all supporting project deliverables.

### 8.3 Project Issue Resolution

From time to time, a FSO-reported defect may be rejected by ATIMS for a number of reasons including but not limited to:

- a) The defect is actually a change to the intended design. A minor change is called a “Design Improvement” where the FSO needs a small adjustment in order to make the system work for their purposes.

## Exhibit A

- b) The Defect is not a software defect but is a training, configuration, setup or other non-software requirement and is the responsibility of the FSO to resolve.
- c) The Defect is not clearly defined, the steps to reproduce are not defined, and ATIMS cannot reproduce the Defect on our test systems, or the FSO has not tied the Defect back to a clearly defined Requirement.
- d) The Defect solution requires or will drive new client requirements.

The ATIMS PM will track these issues; however, the item will be reviewed and negotiated at the business level within ATIMS, according to the escalation path set out below:

	ATIMS	FSO
Level 3	Felix Rabinovich, Vice-President	FSO Executive Sponsor
Level 2	Ankit Vankamamidi, PMO Manager	FSO PMO
Level 1	ATIMS Project Manager	FSO PM

If agreement cannot be reached through this process, the terms of the Agreement shall prevail. All other work and processes will proceed in isolation of the Project Issue until the Project Issue is resolved and re-instated into the Project Schedule.

## 8.4 Defect Severity and Definition

Severity Level	Definition
1 - Urgent	<p>Critical defect resulting in total failure of software, loss of data, hardware failure, safety issue or in which a requirement is not met and there is no feasible workaround and testing cannot continue on other test cases due to the defect.</p> <p>Examples:</p> <ul style="list-style-type: none"> <li>a) Major system failure; no users can login or use the application at all.</li> <li>b) The system crashes or freezes completely when a particular action is executed.</li> </ul>
2 – Very High	<p>Defect in which a requirement or functionality is not met and there is no acceptable workaround.</p> <p>Examples:</p> <ul style="list-style-type: none"> <li>a) The intake screen errors when trying to enter an inmate resulting in the user being unable to create an intake record. There is no possible work around to create the intake record another way.</li> <li>b) A mandatory field in a record will not allow entry of data into it and therefore the record as a whole cannot be saved. There is no work around.</li> </ul>
3 – High	<p>Defect in which a requirement or functionality is not met but an acceptable workaround is available.</p> <p>Examples:</p> <ul style="list-style-type: none"> <li>a) A date field does not default the current date as detailed in the design, but the user can manually go and select a date.</li> <li>b) Scheduled report does not email automatically as configured; however, report can be manually run by user and sent via email as attachment.</li> </ul>
4 – Medium	<p>Defect in which the fault or limitation does not materially affect the operation of the system or the business process in which it is identified.</p> <p>Examples:</p> <ul style="list-style-type: none"> <li>a) On completion of a wizard step, the next button has to be clicked 2 times by the user before they can continue.</li> <li>b) The sort order of a row of records is incorrect.</li> </ul>
5 – Low	<p>Defect of minor significance where formatting, spelling or cosmetics are incorrect.</p> <p>Examples:</p> <ul style="list-style-type: none"> <li>a) Spelling mistake on a field label.</li> <li>b) Spacing between columns is irregular.</li> <li>c) Wrong date format.</li> </ul>

## **9 System Documentation**

ATIMS shall provide user manuals of sufficient depth and clarity to enable users to utilize all relevant system features in the course of their work duties.

ATIMS shall provide technical documentation of sufficient depth and clarity to enable FSO IT or FSO technical personnel to understand the underlying structure and function of system components, to troubleshoot the application software and interfaces, to support users, to perform all system administration and operation duties, and to plan for potential future integration with other applications.

ATIMS shall populate on-line help content consistent with documentation provided under this task.

ATIMS shall provide documentation specific to the FSO's JMS implementation.

## **10 Release Implementation**

ATIMS shall assess the readiness of FSO IT or FSO provided technical infrastructure. ATIMS shall provide notice to the FSO of any technical infrastructure deficiencies.

ATIMS shall plan and conduct activities required to begin production use of the JMS. ATIMS shall install all application components, establish the initial system configuration, load initial data per the Data Conversion Plan and perform any other activities required for production usage of the JMS. ATIMS shall support the FSO for any cutover activities restricted to FSO staff. ATIMS shall test the production system prior to system go-live.

ATIMS shall provide on-site Release Implementation Support for 5 calendar days after the cutover. ATIMS shall provide on-site support at all custody locations during this period.

ATIMS shall conduct one (at a minimum) Table Top Rehearsal cutover to confirm the process and to establish the cutover timeline.

ATIMS shall provide multiple cutover cycles if specified in the Deployment Strategy deliverable.

ATIMS shall update the Configuration Management Plan with the go-live production configuration.

## **11 Post Release Implementation Support**

ATIMS Software Support and Maintenance Agreement provides customers with fixes, upgrades and updates to licensed Software released during the Maintenance period. As part of keeping your ATIMS InCustody JMS Annual Maintenance & Support Agreement current, additional services are included as part of the annual fee negotiated with the FSO. These services can include Annual



Training, and/or Form, Report and Interface Development Services. The value of a service category description (training, form, report, etc.) can be used towards another category in that year's allotment, as long as the total cost does not exceed the allowable amount (with the different hourly cost/value).

ATIMS shall provide maintenance and support of the production JMS for a period of one year as warranted. Maintenance in subsequent years shall be provided for the term of this Agreement as long as the County is current on annual maintenance payments specified in Exhibit B. ATIMS's services shall include (at a minimum):

- A. Provision of core JMS upgrades, including enhancements and new features
- B. Level 2 help desk support
- C. Defect correction
- D. Impact analysis of upcoming patches and upgrades
- E. Modifications to ATIMS provided components and configurations to support upcoming patches and upgrades
- F. Testing and deployment of patches and upgrades in all FSO environments
- G. Periodic health checks of the production system
- H. Ongoing tuning and other required system level administration
- I. Recommendations for infrastructure upgrades
- J. Application modifications required to support scheduled infrastructure upgrades

ATIMS shall support the FSO to apply maintenance and support activities to components restricted for access to FSO staff.

ATIMS shall recommend and support infrastructure (e.g., operating system, database, etc.) upgrades such that the utilized infrastructure is no more than two major releases behind the current release available from the provider of the infrastructure component.

ATIMS shall bill the FSO for maintenance and support services provided after the acceptance of the final Cutover Completion Report. If the JMS is implemented incrementally as specified in the Deployment Strategy, ATIMS shall provide maintenance and support services for the incremental releases at no additional cost to the FSO.

ATIMS shall be subject to the following response requirements for production issues reported by the FSO:

## Exhibit A

Level	Level Definition	Response Requirement
Level 1	<p>An error, malfunction or other deficiency that meets both of the following criteria:</p> <p>(i) The deficiency significantly impairs the FSO normal business operations; diminishes employee safety or well-being; exposes the FSO to significant liability or risk; significantly increases the cost, decreases the value, or impedes the efficiency of the FSO resources or operations; or significantly inconveniences the FSO’s customers.</p> <p>(ii) No workaround is currently developed, implemented, and accepted to alleviate the deficiency’s impact.</p>	<p>ATIMS shall begin taking action toward a resolution within a time period of one (1) hour. Contractor shall use continuous best effort until the problem is resolved.</p>
Level 2	<p>An error, malfunction or other deficiency that meets both of the following criteria:</p> <p>(i) The deficiency causes substantial inconsistencies, irregularities, inefficiencies, or potential for mistakes, but does not meet the criteria for a Level I Priority.</p> <p>(ii) No workaround is currently developed, implemented and accepted to alleviate the deficiency’s impact.</p>	<p>ATIMS shall begin taking action toward a resolution within a time period of two (2) hours. Contractor shall provide ongoing and diligent action to correct the deficiency</p>
Level 3	<p>An error, malfunction or other deficiency that does not meet the criteria for Level I or Level II Priority, but causes system response time to fall below fifty percent (50%) of system response time requirements for more than four (4) hours per month</p>	<p>ATIMS shall successfully implement a resolution within a time period of thirty (30) days.</p>
Level 4	<p>An error, malfunction or other deficiency that has little or no immediate impact on the FSO / FSO’s business operations, costs, risks, employees, or customers, but is desirable for the long-term viability and utility of the system</p>	<p>ATIMS shall successfully implement a resolution within a time period of ninety (90) days.</p>

ATIMS shall provide additional support services at the direction of the FSO and at additional cost. The table below is taken from the ATIMS Support and Maintenance Guide; it indicates which services are included in this Agreement along with the ATIMS business unit responsible for the support.

## Exhibit A

Service Agreement  
Statement of Work:

Page 20

Description	Software Support and Maintenance	Professional Services
<b>Upgrades and updates</b>		
Supply new software version	✓	
Install new software version	✓	
System reinstall — application malfunction	✓	
System reinstall — hardware/network problem		✓
<b>Support/bugs/errors</b>		
Business hours Tier 1 support	✓	
24/7 critical after-hour support	✓	
Problem with application/malfunction	✓	
Code testing and replication of errors	✓	
Simulation of client environment	✓	
Data discovery due to malfunction	✓	
Problem with internal hardware/network		✓
<b>Environment</b>		
Database optimization – indexing	✓	
Creation of additional databases	✓	
Replication of database environment	✓	
Installation of additional environments		✓
Reinstallation of new server or configuration		✓
Database maintenance – backups		✓
Data mining/data discovery request		✓
<b>Customization / Enhancements</b>		
Consultation for customization or enhancement — up to one (1) hour	✓	
Software configuration using database settings	✓	
Creation of additional custom forms		✓
Creation of additional custom reports		✓
Client-initiated customization/enhancement		✓
<b>Interfaces</b>		
Consultation for third-party software interface — up to one (1) hour	✓	
Consultation for third-party software interface — beyond one (1) hour		✓
Development of third-party interfaces		✓
<b>Training</b>		
User manuals	✓	

# Exhibit A

Service Agreement  
Statement of Work:

---

Page 21

Description	Software Support and Maintenance	Professional Services
User group InCustody webinars	✓	
Additional client-requested training		✓
Training on new software functionality		✓

## 12 Required Interfaces / Exchanges

Vendor / Need	Agency Description	ATIMS Exchange Options	ATIMS Assumption	Effort / Pricing (based on Option selected)
Numi / Debit Cards	<p>Inmate debit card system. FSO requires an outbound interface to core JMS. Generates a debit card for inmate remaining balances at time of inmate discharge.</p> <p>NUMI Financials interface Provide Cash Card with Left over balance on the inmate accounts and make zero balance in the JMS system</p>	Event Based Export	<p>Export - ATIMS assumes that the County will be using ATIMS money system for banking. ATIMS will integrate with NUMIs debt card system to allow issuing of debit cards. Please note that this is only for the interface of the solution, the debit card themselves and account management are provided by NUMI. In the interface ATIMS has an option to allow DEBIT CARD transactions. This button will trigger an event that will be configured to call NUMIs web-based REST service to "LOAD" the card with the transaction amount. There are checks and balance in place to prevent re-use of cards, etc. ATIMS will also offer a void card transaction which will send a different message to NUMI to cancel a card. This solution can replace check writing or be used in conjunction with check writing and/or cash return.</p>	LOE: 7 days
VINES / Victim Services	Victim Services systems that notify pre-defined witnesses and/or victims associated with the Inmate that they are to be released	Interval & Daily Export	(1) Outbound Roster - ATIMS assumes a standardized approach for interfacing with Vine. The interface uses combination of event-based export and nightly run for a re-sync once a day. The event-based export will export one inmate at a time with basic Inmate and Release Data that has already been agreed upon between the ATIMS and VINE. Additional data such Demographics and Case and Charges is not included. The events will be triggered based on events needed by the vendor such as Intake, Booking	(1) LOE: 3 days

## Exhibit A

Vendor / Need	Agency Description	ATIMS Exchange Options	ATIMS Assumption	Effort / Pricing (based on Option selected)
		Event based or Nightly Run	<p>Complete, Release, Housing Change... The output of the event-based export will be XML sent to a SFTP folder. The nightly run will be a re-sync file of all active inmates and recent releases using the same xml structure. The output of the nightly run will also be a XML sent to a SFTP folder.</p> <p>(2) Outbound Photo - Based on Booking Complete Event or Nightly run of the active roster, ATIMS will send a binary base 64 stream a County REST web service, the binary stream will be as part of the payload data within the tag itself. As an alternative approach ATIMS can also create an XML file to a UNC or FTP/SFTP folder using XML and place the binary stream within the file. Please note: that ATIMS will NOT copy the file itself to a destination, only the binary of the photo will be sent within interface work</p>	(2) LOE: 5 days
Canteen	System to support the management and distribution of food and goods to Inmates Canteen interface is two-way interface, receive files and push data to the Database. Send file to canteen current balances.	Interval Export	<p>(1) Outbound Roster #1 - ATIMS assumes an export a complete active roster, with revoke commissary privilege. Additional restrictions based on flags are not included. The roster will be triggered from a scheduler running a timed interval such as every 15 minutes. The output of the export can be ACSII text delimited or fixed length, XML or JSON. The destination folder can be a UNC path or an FTP/SFTP folder using any of the formats. As an alternative to the destination folder, the export can also go to a REST Post Web Service using JSON or XML payload.</p> <p>&lt;or&gt;</p>	(1) LOE: 3 days  (2) LOE: 4 days

## Exhibit A

Service Agreement  
Statement of Work:

Vendor / Need	Agency Description	ATIMS Exchange Options	ATIMS Assumption	Effort / Pricing (based on Option selected)
	DEPENDS ON TRANSACTION MGMT, PER THESE OPTIONS, NOT DONE IN ATIMS INMATE MONEY MODULE	<p>Event Based Report</p> <p>Web Service Host or File Folder Watch</p>	<p>(2) Outbound Roster #2- ATIMS assumes event-based exporting of an inmate data with revoke commissary privilege. Additional restrictions based on flags are not included. The events will be triggered based on events needed by the vendor such as Intake, Booking Complete, Release, Name Change, Demographic Change, Housing Change roster, etc... The output of the export can be ACSII text delimited or fixed length, XML or JSON. The destination folder can be a UNC path or an FTP/SFTP folder using any of the formats. As an alternative to the destination folder, the export can also go to a REST Post Web Service using JSON or XML payload.</p> <p>(3) Inbound balance - ATIMS will accept an inbound REST web service POST message with inmate balance data payload OR will schedule a folder watch to consume a file with balance data. The payload will be mapped and update the inmate's current balance to reflect the same amount in the commissary system. Transactional accounting data is not included, strictly the ending balance</p>	(3) LOE: 5 days
TouchPay	System to support the ability to deposit money into an Inmate's Account by an individual external to the FSO	<p>Interval Export</p> <p>Web Service Host or</p>	<p>(1) Outbound Roster #1 – ATIMS assumes an export a complete active roster, with inmate's schedule and/or revoke privilege. The roster will be triggered from a scheduler running a timed interval such as every 5 minutes. The output of the export can be ACSII text delimited or fixed length, XML or JSON. The destination folder can be a UNC path or an FTP/SFTP folder using any of the formats. As an alternative to the destination folder, the export can also go to a REST Post Web Service using JSON or XML payload.</p>	

## Exhibit A

Service Agreement  
Statement of Work:

Vendor / Need	Agency Description	ATIMS Exchange Options	ATIMS Assumption	Effort / Pricing (based on Option selected)
	Touch pay interface Receive deposited information to pull every 5 minutes	File Folder Watch	(2) Inbound – ATIMS will accept a transaction file the output of the export can by ACSII text delimited or fixed length, XML or JSON. The destination folder can be a UNC path or an FTP/SFTP folder using any of the formats. As an alternative to the destination folder, the export can also go to a REST Post Web Service using JSON or XML payload	
SafetyCheck / Guardian RFID	TBD		ATIMS Officer Mobile to be considered to replace the need for this interface.	

[Additional interfaces identified for consideration during discover (Fit and gap analysis).

Vendor / Need	Agency Description	ATIMS Exchange Options	ATIMS Assumption	Effort / Pricing (based on Option selected)
Biometrics (Livescan)	A biometric search engine that enables FSO users to investigation biometric data such as fingerprints	Event Based Export	(1) Outbound Booking – 10 Print – Single Pass Approach (Livescan) - ATIMS assumes event-based exporting of a Person data, Booking data, Case Data and Charge Data. The assumption is a single pass to prepopulate data elements within the Livescan 10 print process. ATIMS will link the SEND TO LIVELSCAN button to the export and configure the format based on the vendors specification to a UNC output or FTP/SFTP folder or a REST web service. The file can then be accessed from the Livescan	(1) LOE – 4 days



## Exhibit A

Service Agreement  
Statement of Work:

---

Vendor / Need	Agency Description	ATIMS Exchange Options	ATIMS Assumption	Effort / Pricing (based on Option selected)
*Required for Dual Pass*		Event Based Export	terminal to pre-populate the livescan data to prevent dual entry. ATIMS will format to vendors specification if the results are in XML, JSON, ASCII text. Any format that needs to be created with a binary specification is not included. If using a REST Post Web Service ATIMS assumes standard JSON or XML payload <or> (2) Outbound Booking – 10 Print – Dual Pass Approach - ATIMS assumes event-based exporting in 2 phases. The 1st phase is to identify the inmate, the 2nd phase is to upload the charges. In the 1st phase ATIMS will link the creation of an INTAKE event and send Person data, Livescan will prepopulate only the person and then completes the 10-print without charge data. This 1st pass assumes the response in an INBOUND interface using for VERIFY ID (Verify ID is a process in ATIMS which compares identifying numbers such as state, federal and/or local AFIS numbers). The 2nd pass assumes that identity has been verified. ATIMS will configure BOOKNG COMPLETE event to send the correct Identification for the booking number along with the case and charge data. Both outbound passes are	(2) LOE: 15 days
		Web Service Host or File Folder Watch	export based on the vendors specification to a UNC output or FTP/SFTP folder or a REST web service. ATIMS will format to vendors specification if the results are in XML, JSON, ASCII text. Any format that needs to be created with a binary specification is not included. If using a REST Post Web Service ATIMS assumes standard JSON or XML payload.	(3) LOE: 8 days

## Exhibit A

Service Agreement  
Statement of Work:

Vendor / Need	Agency Description	ATIMS Exchange Options	ATIMS Assumption	Effort / Pricing (based on Option selected)
			<p>(3) Inbound Verify ID (Option for Single Pass) - ATIMS will accept an inbound interface with Booking Number (Pass-through) Number and Identifying Numbers such as the state number, federal number and optionally local AFIS number. Typically, these numbers are referred to as SID, FBI and AFIS number respectively. The same can be accomplished using a folder watch to consume a file with the same data. ATIMS will use the Booking Number for matching the record and the Identifying Numbers to automatically run the ATIMS Verify Id API. This will set the inmate as VERIFIED, MERGE or MOVE state so that records can fix any issues if the person is not verified in the Verify ID queue. Typically, this data will come from the state switch or livescan vendor, the County must provide this data to ATIMS in a parsed state. ATIMS assumes a REST Web Service Host to provide an inbound POST message for the payload OR folder watch text file in ASCII, standard XML or JSON, any other formatting including binary specification is not included.</p>	
AFIS / PreBook Probable Cause	PBPC Module - Livescan or AFIS or Mobile ID Vendor (2 print)		<p>Inbound Identity – 2 biometric read - Prior to the creation of Intake, ATIMS will accept an inbound REST web service POST message with Name, DOB and Identifying Numbers such as at the state number, federal number and optionally the AFIS county number. Typically, these numbers are referred to as SID, FBI and AFIS number respectively. The same can be accomplished using a folder watch to consume a file with the same data. ATIMS will place the read of the fingerprint in a staging location. The Identity acceptance will use the staging to match and accept the person based on the biometric read.</p>	LOE: 5 days

## Exhibit A

Service Agreement  
Statement of Work:

Vendor / Need	Agency Description	ATIMS Exchange Options	ATIMS Assumption	Effort / Pricing (based on Option selected)
			Please note: The County must provide this data to ATIMS in a parsed state, binary format is not included. Typically, this data will come from either the AFIS vendor, Livescan Vendor or any 3rd party mobile ID having access to the states biometric system. The solution for the biometric matching during intake is pre-packaged within ATIMS, only the interface to accept the biometric read is needed	
ViaPath / Inmate Phones	Once an Inmate receives a housing / bed assignment, FSO sends information to indicate that an Inmate is in FSO custody	Interval Export           Event Based Report	(1) Outbound Roster #1 - ATIMS assumes an export a complete active roster. The roster will be triggered from a scheduler running a timed interval such as every 15 minutes. The output of the export can by ACSII text delimited or fixed length, XML or JSON. The destination folder can be a UNC path or an FTP/SFTP folder using any of the formats. As an alternative to the destination folder, the export can also go to a REST Post Web Service using JSON or XML payload  (2) Outbound Roster #2 - ATIMS assumes event-based exporting of an inmate data. The events will be triggered based on events needed by the phone vendor such as Intake, Booking Complete, Release, Name Change, Demographic Change, Housing Change roster, etc... The output of the export can by ACSII text delimited or fixed length, XML or JSON. The destination folder can be a UNC path or an FTP/SFTP folder using any of the formats. As an alternative to the destination folder, the export can also go to a REST Post Web Service using JSON or XML payload	(1) LOE: 3 days           (2) LOE: 4 days

## Exhibit A

Service Agreement  
Statement of Work:

Vendor / Need	Agency Description	ATIMS Exchange Options	ATIMS Assumption	Effort / Pricing (based on Option selected)
ViaPath / Video Visitation	System enabling Inmates to participate in visits via a video teleconference	Interval Export	<p>(1) Outbound Roster #1 – ATIMS assumes an export a complete active roster, with inmate’s schedule and/or revoke privilege. The roster will be triggered from a scheduler running a timed interval such as every 15 minutes. The output of the export can by ACSII text delimited or fixed length, XML or JSON. The destination folder can be a UNC path or an FTP/SFTP folder using any of the formats. As an alternative to the destination folder, the export can also go to a REST Post Web Service using JSON or XML payload</p>	(1) LOE: 4 days
		Event Based Export	<p>(2) Outbound Roster #2 – ATIMS assumes event-based exporting of an inmate data, with reserved schedule and/or revoke privilege. The events will be triggered based on events needed by the vendor such as Intake, Booking Complete, Release, Name Change, Demographic Change, Housing Change roster, etc... The output of the export can by ACSII text delimited or fixed length, XML or JSON. The destination folder can be a UNC path or an FTP/SFTP folder using any of the formats. As an alternative to the destination folder, the export can also go to a REST Post Web Service using JSON or XML payload</p>	(2) LOE: 5 days
		Web Service Host or File Folder Watch	<p>(3) Inbound Appointment (Optional) - ATIMS will accept an inbound REST web service POST message with appointment data payload OR will schedule a folder watch to consume a file with appointment data. The payload will be mapped new appointment assigned to an inmate’s schedule</p>	(3) LOE: 5 days

## Exhibit B

### Compensation

The Contractor will be compensated for performance of its services under this Agreement as provided in this Exhibit B. The Contractor is not entitled to any compensation except as expressly provided in this Exhibit B.

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

## Exhibit B – Compensation



### SECTION I - ONE TIME COST

Date: 01OCT2023

Description	Proposed Price
1. Software Licensing <sup>5</sup>	\$ 1,335,600
2. Hardware <i>(total from Section II below)</i> <sup>2</sup>	\$ -
3. Hosting, Network & Storage <sup>1</sup>	N/A
4. Interfaces <sup>4</sup>	\$ 44,800
5. Installation/Implementation <sup>3</sup>	\$ 779,512
6. Project Management	\$ 174,720
7. Training, including all materials	\$ 105,000
8. Other One-Time Costs <i>(total from Section III TAB)</i>	\$ -
9. Hardware or Software Costs subsequently identified during gapfit analysis <sup>6</sup>	\$ 236,400
	<b>\$ 2,676,032</b>

PROPOSER NAME: The ACT-1 Group, Inc. dba ATIMS

Assumptions:

<sup>1</sup> Hosting, network & storage are managed by the Agency for an on-premise Solution. ATIMS will work closely with the Agency to provide specifications and meet this need.

<sup>2</sup> - ATIMS typically recommends that the Agency procure its own hardware as it will get better pricing and the warranty will be direct from the vendor. ATIMS has provided budgetary pricing per item to help prepare the project budget. The exception to this is the Embedded Mugshot Camera Add-on License - 1 camera, associated hardware and installation are included in the Cloud Annual SaaS cost.

<sup>3</sup> installation & implementation includes the following activities/roles: Business Analysis; Application configuration, Form Development, Report Development; Data Conversion; Project Documentation, Test / Quality Control and Travel.

<sup>4</sup> Interfaces for this project include: Canteen, Numi, touchpay, and VINE.

<sup>5</sup> ATIMS Licenses includes the On-Premise JMS license & any add-on functional licenses selected (biometrics, \*embedded mugshot camera, \*inmate self service capabilities). The 2 add-on licenses with \* were added on 7/25/24 per T Burgamy request; external website add-on license was removed 8/13/24

<sup>6</sup> Customization, what ATIMS calls enhancements are changes to software code and included in the 1 Annual Cost provided on IV - Recurring. They are not considered a Professional Implementation Services cost. ATIMS is recommending our MOBILE APPLICATION to replace the RFID need (and associated interfaces) if the Agency has wifi available throughout the facility(ies); to be considered as part of gapfit

## Exhibit B – Compensation

### Implementation Milestone Payment Plan for 1st 2 Year of Contract (1-Time Costs)

	Milestone Amount	
<b>1 Contract Initiation</b>	<b>\$267,603</b>	<b>10%</b>
<u>Deliverables:</u>		
Approved Baseline Project Schedule		
Approved SOW		
Approved Requirements Tracking Matrix (RTM)		
Approved and signed contract		
<b>2 Project Planning</b>	<b>\$80,281</b>	<b>3%</b>
<u>Deliverables:</u>		
Approved Project Management Plan/Schedule		
Approved Requirements Management Plan		
Approved System Testing Plan		
Approved Interface Management Plan		
Communications Plan		
Approved Training Plan		
Kick-Off meeting		
<b>3 Jail Management System: Analysis, Development, &amp; Testing</b>	<b>\$53,521</b>	<b>2%</b>
<u>Deliverables:</u>		
Pre-Implementation Analysis		
Requirements Validation		
Conceptual Design Document		

## Exhibit B – Compensation

<b>4</b>	<b>Base Product Implementation: Test Environment</b> Base Product Installation (ERD, Data Dictionary) - JMS Complete Requirements Review Complete Enhancement Identification	<b>\$133,802</b>	<b>5%</b>
<b>5</b>	<b>Jail Management System: Interfaces</b> <u>Deliverables:</u> Approved Interface Management Requirements Interface Control Documents for each interface Implement Mandatory Interfaces: Production Environment	<b>\$535,206</b>	<b>20%</b>
<b>6</b>	<b>Jail Management System: Data Migration</b> <u>Deliverables:</u> Approved Data Migration Plan Initial Data Conversion Delivery Approved Data Conversion Validation	<b>\$535,206</b>	<b>20%</b>
<b>7</b>	<b>Jail Management System: Enhancement Development and User Acceptance Testing</b> <u>Deliverables:</u> Work on Enhancements Items Enhancement complete including completion of custom requirement builds and Form creation System functionality validated through the use of requirements defined within the Traceability Matrix attachments UAT Complete	<b>\$267,603</b>	<b>10%</b>



## Exhibit B – Compensation

<b>8</b>	<b>Reporting</b> <u>Deliverables:</u> Core reports created Core reports UAT complete	<b>\$133,802</b>	5%
<b>9</b>	<b>Jail Management System: Production Environment</b> <u>Deliverables:</u> Completed Training Test and Production Environments Approved Go-Live Plan Go Live	<b>\$669,008</b>	25%
<b>10</b>	<b>Post Go Live</b> Move to ongoing support Sunsetting of replaced systems: Final solution acceptance by County		
<b>Implementation Cost</b>		<b>\$2,676,032</b>	

NOTES: 1. Cloud subscription annual cost not included  
 2. Travel Expenses (not to exceed \$99,512 per response) will be billed as incurred

## Exhibit B – Compensation



Date: 01OCT2023

**SECTION II - HARDWARE COSTS <OPTIONS> - Provided for Budgetary Purposes ONLY, cost not included in this Agreement**

Description	Cost	Qty	Price
Officer Mobile Tablet(s) - requires wifi	\$ 150		
Inmate Mobile/Pod Tablet(s) - requires wifi	\$ 150		
Signature Pads (Topaz or other...)	\$ 250		
Biometrics readers (Digital Persona or Futronics FS88) [Not sure required / or Category 6 I/J]	\$ 125		
Wristbands (1 box / 500)	\$ 250		
Wristband Sealer	\$ 350		
Digital Imaging [Embedded] Mugshot Camera - Video Capture Machine License + Picturelink Hardware (Uniform background; Setup Kit; S&H) + Canon EOS Rebel T5i w/18-135mm lens + Pan & Tilt Model 340 w/20' cable (SMT); digital mount kit; digital lighting components. Remote Expert Services (Install/Training; Technical Services; Project Mgmt Services).NOTE: If no Pan&Tilt -(\$250) <sup>1</sup>	\$INCL in Add-On Subscription Cost		
<sup>1</sup> Annual Support & Maintenance Fee includes use of software, functional add-on licenses (biometrics, mugshot, self-service) <sup>2</sup> , enhancements <sup>1</sup> and annual support allotment			
<b>Total</b>	<b>\$ NOT INCL 0</b>		<b>\$ -</b>

<sup>1</sup>The Embedded Mugshot Camera Add-on Functional License includes 1 mugshot camera, associated paraphernalia and installation. - cost included in license roll up to annual cloud cost

No other hardware is included in this proposal/project. The costs above are provided to help the County budget as applicable.

## Exhibit B – Compensation



Date: 01OCT2023

PROPOSER NAME: ATIMS, division of The ACT-1 Group, Inc.

SOLUTION: On-Premise / Agency Hosted & Managed

AGENCY: Fresno County Sheriff's Office

ONE TIME COSTS	Proposed Price
Section I - One Time Costs	\$ 2,676,032
Section II - Hardware	\$ -
Section III - Other One Time Costs	\$ -
<b>TOTAL - ONE TIME COSTS</b>	<b>\$ 2,676,032</b>


RECURRING COSTS (10 Years)	PROPOSED
Section IV - ATIMS Annual Support & Maintenance	\$ 2,795,515
<sup>1</sup> Annual Support & Maintenance Fee includes use of software, functional add-on licenses (biometrics, mugshot, self-service) <sup>2</sup> , enhancements <sup>1</sup> and annual support allotment	
<b>TOTAL ALL PHASES - RECURRING (10 YRS)</b>	<b>\$ 2,795,515</b>

<b>GRAND TOTAL ALL PHASES</b>	<b>\$ 5,471,547</b>
-------------------------------	---------------------

## Exhibit B – Compensation

ATIMS, division of The ActOne Group, Inc.  
 SOLUTION: On Premises (Managed & Hosted by Agency)  
 AGENCY: Fresno County Sheriff's Office  
 ANNUAL PAYMENTS DUE - 10 YEAR PERIOD

Date: 30SEP2024



SECTION IV - RECURRING ANNUAL COSTS

**AGENCY: Fresno County Sheriff's Office**

Description	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Year 8	Year 9	Year 10	TOTALS
<b>1. Software License Fee</b>	Implementation	Implementation	Warranty	\$ 376,030	\$ 383,551	\$ 391,222	\$ 399,046	\$ 407,027	\$ 415,168	\$ 423,471	\$ 2,795,515
<b>Total OnGoing Annual Cost</b>	\$ -	\$ -	\$ -	\$ 376,030	\$ 383,551	\$ 391,222	\$ 399,046	\$ 407,027	\$ 415,168	\$ 423,471	\$ 2,795,515

PROPOSER NAME: The ACT-1 Group, Inc. dba ATIMS

Assumptions:  
<sup>1</sup> Annual Support & Maintenance Fee includes use of software, functional add-on licenses (biometrics, mugshot, self-service)<sup>5</sup>, enhancements<sup>6</sup> and annual support allotment

List of Enhancements that require software code changes -  
 TBD as part of GapFit analysis

PROPOSER NAME: The ACT-1 Group, Inc. dba ATIMS

Assumptions:  
<sup>1</sup> Annual Support & Maintenance Fee includes use of software, functional add-on licenses (biometrics, mugshot, self-service)<sup>2</sup>, enhancements<sup>1</sup> and annual support allotment  
 List of Enhancements that require software code changes- TBD as part of GAPFIT analysis.

## Exhibit B – Compensation



Date: 01OCT2023

### SECTION V - VALUE ADDED PRODUCTS / SERVICES

Description	Price
RECOMMENDED:	
1) Embedded Mugshot Camera (Included in the Implementation Costs)	\$ 15,000.00
2) Inmate Lookup External Website (Not included in the Agreement)	\$ 35,000.00
3) Inmate Self Service Functionality (Included in the Implementation Costs)	\$ 30,000.00
<b>Total</b>	<b>\$ 80,000.00</b>

Assumptions: #1 and #3 included in Annual SaaS Cost

1) Embedded Mugshot Camera - The Mugshot Photo is taken using DISI software and controlled camera, is embedded into ATIMS software. The mugshot is attached to JMS and integrates with inmate intake and booking functionality.

2) Inmate Lookup External Website - The Mugshot Photo is taken using DISI software and controlled camera, is embedded into ATIMS software. The mugshot is attached to JMS and integrates with inmate intake and booking functionality.

3) Inmate Self Service Functionality - ATIMS base tablet/kiosk application includes secure Booking, Visitation, Appointments, Incident, and Grievance information. In addition, it allows the inmates to place requests and receive responses. \*This can also be added to a commissary or phone vendors POD Kiosk or tablet. \*\*Kiosk hardware is typically procured through the Commissary or Trust Accounting Vendor.

## Exhibit B – Compensation

Date: 01OCT2023



Annual Allotment of Service Hours	Total Annual Hours	Hourly Cost (0800-1700)	Total Available Cost
Desired Service TBD	160	\$ 200	\$ 32,000
TOTAL			\$ 32,000

These included hours can be used towards any service (configuration, interface development, form development, or training that your Agency might need. The hours do not roll over and would be available for 1 calendar year from the date of System Approval post Go Live.

## Exhibit C

### Self-Dealing Transaction Disclosure Form

In order to conduct business with the County of Fresno ("County"), members of a contractor's board of directors ("County Contractor"), must disclose any self-dealing transactions that they are a party to while providing goods, performing services, or both for the County. A self-dealing transaction is defined below:

"A self-dealing transaction means a transaction to which the corporation is a party and in which one or more of its directors has a material financial interest."

The definition above will be used for purposes of completing this disclosure form.

#### Instructions

- (1) Enter board member's name, job title (if applicable), and date this disclosure is being made.
- (2) Enter the board member's company/agency name and address.
- (3) Describe in detail the nature of the self-dealing transaction that is being disclosed to the County. At a minimum, include a description of the following:
  - a. The name of the agency/company with which the corporation has the transaction; and
  - b. The nature of the material financial interest in the Corporation's transaction that the board member has.
- (4) Describe in detail why the self-dealing transaction is appropriate based on applicable provisions of the Corporations Code.

The form must be signed by the board member that is involved in the self-dealing transaction described in Sections (3) and (4).

## Exhibit C

<b>(1) Company Board Member Information:</b>			
<b>Name:</b>		<b>Date:</b>	
<b>Job Title:</b>			
<b>(2) Company/Agency Name and Address:</b>			
<b>(3) Disclosure (Please describe the nature of the self-dealing transaction you are a party to)</b>			
<b>(4) Explain why this self-dealing transaction is consistent with the requirements of Corporations Code § 5233 (a)</b>			
<b>(5) Authorized Signature</b>			
<b>Signature:</b>		<b>Date:</b>	



## Exhibit D

### Insurance Requirements

#### 1. Required Policies

Without limiting the County's right to obtain indemnification from the Contractor or any third parties, Contractor, at its sole expense, shall maintain in full force and effect the following insurance policies throughout the term of this Agreement.

- (A) **Commercial General Liability.** Commercial general liability insurance with limits of not less than Two Million Dollars (\$2,000,000) per occurrence and an annual aggregate of Four Million Dollars (\$4,000,000). This policy must be issued on a per occurrence basis. Coverage must include products, completed operations, property damage, bodily injury, personal injury, and advertising injury. The Contractor shall obtain an endorsement to this policy naming the County of Fresno, its officers, agents, employees, and volunteers, individually and collectively, as additional insureds, but only insofar as the operations under this Agreement are concerned. Such coverage for additional insureds will apply as primary insurance and any other insurance, or self-insurance, maintained by the County is excess only and not contributing with insurance provided under the Contractor's policy.
- (B) **Automobile Liability.** Automobile liability insurance with limits of not less than One Million Dollars (\$1,000,000) per occurrence for bodily injury and for property damages. Coverage must include any auto used in connection with this Agreement.
- (C) **Workers Compensation.** Workers compensation insurance as required by the laws of the State of California with statutory limits.
- (D) **Employer's Liability.** Employer's liability insurance with limits of not less than One Million Dollars (\$1,000,000) per occurrence for bodily injury and for disease.
- (E) **Professional Liability.** Professional liability insurance with limits of not less than One Million Dollars (\$1,000,000) per occurrence and an annual aggregate of Three Million Dollars (\$3,000,000). If this is a claims-made policy, then (1) the retroactive date must be prior to the date on which services began under this Agreement; (2) the Contractor shall maintain the policy and provide to the County annual evidence of insurance for not less than five years after completion of services under this Agreement; and (3) if the policy is canceled or not renewed, and not replaced with another claims-made policy with a retroactive date prior to the date on which services begin under this Agreement, then the Contractor shall purchase extended reporting coverage on its claims-made policy for a minimum of five years after completion of services under this Agreement.
- (F) **Technology Professional Liability (Errors and Omissions).** Technology professional liability (errors and omissions) insurance with limits of not less than Two Million Dollars (\$2,000,000) per occurrence and in the aggregate. Coverage must encompass all of the Contractor's obligations under this Agreement, including but not limited to claims involving Cyber Risks.
- (G) **Cyber Liability.** Cyber liability insurance with limits of not less than Two Million Dollars (\$2,000,000) per occurrence. Coverage must include claims involving Cyber Risks. The cyber liability policy must be endorsed to cover the full replacement value of damage to,

## Exhibit D

alteration of, loss of, or destruction of intangible property (including but not limited to information or data) that is in the care, custody, or control of the Contractor.

**Definition of Cyber Risks.** “Cyber Risks” include but are not limited to (i) Security Breach, which may include Disclosure of Personal Information to an Unauthorized Third Party; (ii) data breach; (iii) breach of any of the Contractor’s obligations under Exhibit E of this Agreement; (iv) system failure; (v) data recovery; (vi) failure to timely disclose data breach or Security Breach; (vii) failure to comply with privacy policy; (viii) payment card liabilities and costs; (ix) infringement of intellectual property, including but not limited to infringement of copyright, trademark, and trade dress; (x) invasion of privacy, including release of private information; (xi) information theft; (xii) damage to or destruction or alteration of electronic information; (xiii) cyber extortion; (xiv) extortion related to the Contractor’s obligations under this Agreement regarding electronic information, including Personal Information; (xv) fraudulent instruction; (xvi) funds transfer fraud; (xvii) telephone fraud; (xviii) network security; (xix) data breach response costs, including Security Breach response costs; (xx) regulatory fines and penalties related to the Contractor’s obligations under this Agreement regarding electronic information, including Personal Information; and (xxi) credit monitoring expenses.

### 2. Additional Requirements

(A) **Verification of Coverage.** Within 30 days after the Contractor signs this Agreement, and at any time during the term of this Agreement as requested by the County’s Risk Manager or the County Administrative Office, the Contractor shall deliver, or cause its broker or producer to deliver, to the County Risk Manager, at 2220 Tulare Street, 16th Floor, Fresno, California 93721, or HRRiskManagement@fresnocountyca.gov, and by mail or email to the person identified to receive notices under this Agreement, certificates of insurance and endorsements for all of the coverages required under this Agreement.

- (i) Each insurance certificate must state that: (1) the insurance coverage has been obtained and is in full force; (2) the County, its officers, agents, employees, and volunteers are not responsible for any premiums on the policy; and (3) the Contractor has waived its right to recover from the County, its officers, agents, employees, and volunteers any amounts paid under any insurance policy required by this Agreement and that waiver does not invalidate the insurance policy.
- (ii) The commercial general liability insurance certificate must also state, and include an endorsement, that the County of Fresno, its officers, agents, employees, and volunteers, individually and collectively, are additional insureds insofar as the operations under this Agreement are concerned. The commercial general liability insurance certificate must also state that the coverage shall apply as primary insurance and any other insurance, or self-insurance, maintained by the County shall be excess only and not contributing with insurance provided under the Contractor’s policy.
- (iii) The automobile liability insurance certificate must state that the policy covers any auto used in connection with this Agreement.

## Exhibit D

- (iv) The professional liability insurance certificate, if it is a claims-made policy, must also state the retroactive date of the policy, which must be prior to the date on which services began under this Agreement.
  - (v) The technology professional liability insurance certificate must also state that coverage encompasses all of the Contractor's obligations under this Agreement, including but not limited to claims involving Cyber Risks, as that term is defined in this Agreement.
  - (vi) The cyber liability insurance certificate must also state that it is endorsed, and include an endorsement, to cover the full replacement value of damage to, alteration of, loss of, or destruction of intangible property (including but not limited to information or data) that is in the care, custody, or control of the Contractor.
- (B) **Acceptability of Insurers.** All insurance policies required under this Agreement must be issued by admitted insurers licensed to do business in the State of California and possessing at all times during the term of this Agreement an A.M. Best, Inc. rating of no less than A-: VII.
- (C) **Notice of Cancellation or Change.** For each insurance policy required under this Agreement, the Contractor shall provide to the County, or ensure that the policy requires the insurer to provide to the County, written notice of any cancellation or change in the policy as required in this paragraph. For cancellation of the policy for nonpayment of premium, the Contractor shall, or shall cause the insurer to, provide written notice to the County not less than 10 days in advance of cancellation. For cancellation of the policy for any other reason, and for any other change to the policy, the Contractor shall, or shall cause the insurer to, provide written notice to the County not less than 30 days in advance of cancellation or change. The County in its sole discretion may determine that the failure of the Contractor or its insurer to timely provide a written notice required by this paragraph is a breach of this Agreement.
- (D) **County's Entitlement to Greater Coverage.** If the Contractor has or obtains insurance with broader coverage, higher limits, or both, than what is required under this Agreement, then the County requires and is entitled to the broader coverage, higher limits, or both. To that end, the Contractor shall deliver, or cause its broker or producer to deliver, to the County's Risk Manager certificates of insurance and endorsements for all of the coverages that have such broader coverage, higher limits, or both, as required under this Agreement.
- (E) **Intentionally omitted.**
- (F) **County's Remedy for Contractor's Failure to Maintain.** If the Contractor fails to keep in effect at all times any insurance coverage required under this Agreement, the County may, in addition to any other remedies it may have, suspend or terminate this Agreement upon the occurrence of that failure
- (G) **Subcontractors.** The Contractor shall require and verify that all subcontractors used by the Contractor to provide services under this Agreement maintain insurance meeting all insurance requirements provided in this Agreement. This paragraph does not authorize the Contractor to provide services under this Agreement using subcontractors.

## Exhibit D

This page intentionally left blank.

## Exhibit E – Data Security

### 1. Definitions

Capitalized terms used in this Exhibit E have the meanings set forth in this section 1.

- (A) **“Authorized Employees”** means the Contractor’s employees who have access to Personal Information.
- (B) **“Authorized Persons”** means: (i) any and all Authorized Employees; and (ii) any and all of the Contractor’s subcontractors, representatives, agents, outsourcers, and consultants, and providers of professional services to the Contractor, who have access to Personal Information and are bound by law or in writing by confidentiality obligations sufficient to protect Personal Information in accordance with the terms of this Exhibit E.
- (C) **“County Data”** means all data, information, and other content of any type that is input, imported, interfaced, or processed by County staff into System as a part of this agreement.
- (D) **“Director”** means the County Sheriff’s Finance Bureau Director or his or her designee.
- (E) **“Disclose”** or any derivative of that word means to disclose, release, transfer, disseminate, or otherwise provide access to or communicate all or any part of any Personal Information orally, in writing, or by electronic or any other means to any person.
- (F) **“Person”** means any natural person, corporation, partnership, limited liability company, firm, or association.
- (G) **“Personal Information”** means any and all information, including any data, provided, or to which access is provided, to the Contractor by or upon the authorization of the County, under this Agreement, including but not limited to vital records, that: (i) identifies, describes, or relates to, or is associated with, or is capable of being used to identify, describe, or relate to, or associate with, a person (including, without limitation, names, physical descriptions, signatures, addresses, telephone numbers, e-mail addresses, education, financial matters, employment history, and other unique identifiers, as well as statements made by or attributable to the person); (ii) is used or is capable of being used to authenticate a person (including, without limitation, employee identification numbers, government-issued identification numbers, passwords or personal identification numbers (PINs), financial account numbers, credit report information, answers to security questions, and other personal identifiers); or (iii) is personal information within the meaning of California Civil Code section 1798.3, subdivision (a), or 1798.80, subdivision (e). Personal Information does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.
- (H) **“Privacy”** means the protection of software and data from unauthorized access and manipulation.

## Exhibit E – Data Security

- (I) **“Privacy Practices Complaint”** means a complaint received by the County relating to the Contractor’s (or any Authorized Person’s) privacy practices, or alleging a Security Breach. Such complaint shall have sufficient detail to enable the Contractor to promptly investigate and take remedial action under this Exhibit E.
- (J) **“Security Safeguards”** means physical, technical, administrative or organizational security procedures and practices put in place by the Contractor (or any Authorized Persons) that relate to the protection of the security, confidentiality, value, or integrity of Personal Information. Security Safeguards shall satisfy the minimal requirements set forth in section 3(C) of this Exhibit E.
- (K) **“Security Breach”** means (i) any act or omission that compromises either the security, confidentiality, value, or integrity of any Personal Information or the Security Safeguards, or (ii) any unauthorized Use, Disclosure, or modification of, or any loss or destruction of, or any corruption of or damage to, any Personal Information.
- (L) **“Use”** or any derivative of that word means to receive, acquire, collect, apply, manipulate, employ, process, transmit, disseminate, access, store, disclose, or dispose of Personal Information.

### 2. Standard of Care

- (A) The Contractor acknowledges that, in the course of its engagement by the County under this Agreement, the Contractor, or any Authorized Persons, may Use Personal Information only as permitted in this Agreement.
- (B) The Contractor acknowledges that Personal Information is deemed to be confidential information of, or owned by, the County (or persons from whom the County receives or has received Personal Information) and is not confidential information of, or owned or by, the Contractor, or any Authorized Persons. The Contractor further acknowledges that all right, title, and interest in or to the Personal Information remains in the County (or persons from whom the County receives or has received Personal Information) regardless of the Contractor’s, or any Authorized Person’s, Use of that Personal Information.
- (C) The Contractor agrees and covenants in favor of the County that the Contractor shall:
  - (i) keep and maintain all Personal Information in strict confidence, using such degree of care under this section 2 as is reasonable and appropriate to avoid a Security Breach;
  - (ii) Use Personal Information exclusively for the purposes for which the Personal Information is made accessible to the Contractor pursuant to the terms of this Exhibit E;

## Exhibit E – Data Security

- (iii) not Use, Disclose, sell, rent, license, or otherwise make available Personal Information for the Contractor’s own purposes or for the benefit of anyone other than the County, without the County’s express prior written consent, which the County may give or withhold in its sole and absolute discretion; and
- (iv) not, directly or indirectly, Disclose Personal Information to any person (an “Unauthorized Third Party”) other than Authorized Persons pursuant to this Agreement, without the Director’s express prior written consent.

(D) Notwithstanding the foregoing paragraph, in any case in which the Contractor believes it, or any Authorized Person, is required to disclose Personal Information to government regulatory authorities, or pursuant to a legal proceeding, or otherwise as may be required by applicable law, Contractor shall (i) immediately notify the County of the specific demand for, and legal authority for the disclosure, including providing County with a copy of any notice, discovery demand, subpoena, or order, as applicable, received by the Contractor, or any Authorized Person, from any government regulatory authorities, or in relation to any legal proceeding, and (ii) promptly notify the County before such Personal Information is offered by the Contractor for such disclosure so that the County may have sufficient time to obtain a court order or take any other action the County may deem necessary to protect the Personal Information from such disclosure, and the Contractor shall cooperate with the County to minimize the scope of such disclosure of such Personal Information.

(E) Intentionally omitted.

### 3. Information Security

(A) The Contractor covenants, represents and warrants to the County that the Contractor’s Use of Personal Information under this Agreement does and will at all times comply with all applicable federal, state, and local, privacy and data protection laws, as well as all other applicable regulations and directives, including but not limited to California Civil Code, Division 3, Part 4, Title 1.81 (beginning with section 1798.80), and the Song-Beverly Credit Card Act of 1971 (California Civil Code, Division 3, Part 4, Title 1.3, beginning with section 1747). If the Contractor Uses credit, debit or other payment cardholder information, the Contractor shall at all times remain in compliance with the Payment Card Industry Data Security Standard (“PCI DSS”) requirements, including remaining aware at all times of changes to the PCI DSS and promptly implementing and maintaining all procedures and practices as may be necessary to remain in compliance with the PCI DSS, in each case, at the Contractor’s sole cost and expense.

(B) The Contractor covenants, represents and warrants to the County that, as of the effective date of this Agreement, the Contractor has not received notice of any violation of any privacy or data protection laws, as well as any other applicable regulations or directives, and is not the subject of any pending legal action or investigation by, any government regulatory authority regarding same.

## Exhibit E – Data Security

(C) Without limiting the Contractor's obligations under section 3(A) of this Exhibit E, the Contractor's (or Authorized Person's) Security Safeguards shall be no less rigorous than accepted industry practices and, at a minimum, include the following:

- (i) limiting Use of Personal Information strictly to the Contractor's and Authorized Persons' technical and administrative personnel who are necessary for the Contractor's, or Authorized Persons', Use of the Personal Information pursuant to this Agreement;
- (ii) ensuring that all of the Contractor's connectivity to County computing systems will only be through the County Sheriff's security gateways and firewalls, and only through security procedures approved upon the express prior written consent of the Director;
- (iii) to the extent that they contain or provide access to Personal Information, (a) securing business facilities, data centers, paper files, servers, back-up systems and computing equipment, operating systems, and software applications, including, but not limited to, all mobile devices and other equipment, operating systems, and software applications with information storage capability; (b) employing adequate controls and data security measures, both internally and externally, to protect (1) the Personal Information from potential loss or misappropriation, or unauthorized Use, and (2) the County's operations from disruption and abuse; (c) having and maintaining network, device application, database and platform security; (d) maintaining authentication and access controls within media, computing equipment, operating systems, and software applications; and (e) installing and maintaining in all mobile, wireless, or handheld devices a secure internet connection, having continuously updated anti-virus software protection and a remote wipe feature always enabled, all of which is subject to express prior written consent of the Director;
- (iv) encrypting all Personal Information at advance encryption standards of Advanced Encryption Standards (AES) of 128 bit or higher (a) stored on any mobile devices, including but not limited to hard disks, portable storage devices, or remote installation, or (b) transmitted over public or wireless networks (the encrypted Personal Information must be subject to password or pass phrase, and be stored on a secure server and transferred by means of a Virtual Private Network (VPN) connection, or another type of secure connection, all of which is subject to express prior written consent of the Director);
- (v) strictly segregating Personal Information from all other information of the Contractor, including any Authorized Person, or anyone with whom the Contractor or any Authorized Person deals so that Personal Information is not commingled with any other types of information.



## Exhibit E – Data Security

- (vi) having a patch management process including installation of all operating system and software vendor security patches;
  - (vii) maintaining appropriate personnel security and integrity procedures and practices, including, but not limited to, conducting background checks of Authorized Employees consistent with applicable law; and
  - (viii) providing appropriate privacy and information security training to Authorized Employees.
- (D) During the term of each Authorized Employee's employment by the Contractor, the Contractor shall cause such Authorized Employees to abide strictly by the Contractor's obligations under this Exhibit E. The Contractor shall maintain a disciplinary process to address any unauthorized Use of Personal Information by any Authorized Employees.
- (E) The Contractor shall, in a secure manner, backup daily, or more frequently if it is the Contractor's practice to do so more frequently, Personal Information received from the County, and the County shall have immediate, real-time access, at all times, to such backups via a secure, remote access connection provided by the Contractor, through the Internet.
- (F) The Contractor shall provide the County with the name and contact information for each Authorized Employee (including such Authorized Employee's work shift, and at least one alternate Authorized Employee for each Authorized Employee during such work shift) who shall serve as the County's primary security contact with the Contractor and shall be available to assist the County twenty-four (24) hours per day, seven (7) days per week as a contact in resolving the Contractor's and any Authorized Persons' obligations associated with a Security Breach or a Privacy Practices Complaint.
- (G) The Contractor shall design the System to prevent, to the greatest extent possible, security and privacy breaches, to address contingencies in the event of an unavoidable security or privacy breach, and to provide recovery and backup operation.
- (H) The Contractor shall not knowingly include or authorize any Trojan Horse, back door, time bomb, drop dead device, worm, virus, or other code of any kind that may disable, erase, display any unauthorized message within, or otherwise impair any County computing system, with or without the intent to cause harm. If either County or Contractor becomes aware of the existence of such a malicious program, it shall notify the other Party thereof and Contractor shall promptly remove the malicious program, repair the System and County's data, and repair any other damage done by the malicious program.

### 4. Security Breach Procedures

- (A) Immediately upon the Contractor's awareness or reasonable belief of a Security Breach, the Contractor shall (i) notify the Director of the Security Breach, such notice to be given

## Exhibit E – Data Security

first by telephone at the following telephone number, followed promptly by email at the following email address: (559) 600-8900 / cybersecurity@fresnosheriff.org (which telephone number and email address the County may update by providing notice to the Contractor), and (ii) preserve all relevant evidence (and cause any affected Authorized Person to preserve all relevant evidence) relating to the Security Breach. The notification shall include, to the extent reasonably possible, the identification of each type and the extent of Personal Information that has been, or is reasonably believed to have been, breached, including but not limited to, compromised, or subjected to unauthorized Use, Disclosure, or modification, or any loss or destruction, corruption, or damage.

(B) Immediately following the Contractor's notification to the County of a Security Breach, as provided pursuant to section 4(A) of this Exhibit E, the Parties shall coordinate with each other to investigate the Security Breach. The Contractor agrees to fully cooperate with the County, including, without limitation:

- (i) assisting the County in conducting any investigation;
- (ii) providing the County with physical access to the facilities and operations affected;
- (iii) facilitating interviews with Authorized Persons and any of the Contractor's other employees knowledgeable of the matter; and
- (iv) making available all relevant records, logs, files, data reporting and other materials required to comply with applicable law, regulation, industry standards, or as otherwise reasonably required by the County.

(C) To that end, the Contractor shall, with respect to a Security Breach caused by Contractor's breach of this Agreement, be solely responsible, at its cost, for all notifications required by law and regulation, or deemed reasonably necessary by the County, and the Contractor shall provide a written report of the investigation and reporting required to the Director within 30 days after the Contractor's discovery of the Security Breach.

(D) County shall promptly notify the Contractor of the Director's knowledge, or reasonable belief, of any Privacy Practices Complaint, and upon the Contractor's receipt of that notification, the Contractor shall promptly address such Privacy Practices Complaint, including taking any corrective action under this Exhibit E, all at the Contractor's sole expense, in accordance with applicable privacy rights, laws, regulations and standards. In the event the Contractor discovers a Security Breach, the Contractor shall treat the Privacy Practices Complaint as a Security Breach. Within 24 hours of the Contractor's receipt of notification of such Privacy Practices Complaint, the Contractor shall notify the County whether the matter is a Security Breach, or otherwise has been corrected and the manner of correction, or determined not to require corrective action and the reason for that determination.

## Exhibit E – Data Security

- (E) The Contractor shall take prompt corrective action to respond to and remedy any Security Breach caused by its breach of this Agreement and take mitigating actions, including but not limiting to, preventing any reoccurrence of the Security Breach and correcting any deficiency in Security Safeguards as a result of such incident, all at the Contractor's sole expense, in accordance with applicable privacy rights, laws, regulations and standards. The Contractor shall reimburse the County for all reasonable costs incurred by the County in responding to, and mitigating damages caused by, any such Security Breach, including all costs of the County incurred relation to any litigation or other action described section 4(E) of this Exhibit E.
- (F) The Contractor agrees to cooperate, at its sole expense, with the County in any litigation or other action to protect the County's rights relating to Personal Information, including the rights of persons from whom the County receives Personal Information.

### 5. Oversight of Security Compliance

- (A) The Contractor shall have and maintain a written information security policy that specifies Security Safeguards appropriate to the size and complexity of the Contractor's operations and the nature and scope of its activities.
- (B) Upon the County's written request, to confirm the Contractor's compliance with this Exhibit E, as well as any applicable laws, regulations and industry standards, the Contractor grants the County or, upon the County's election, a third party on the County's behalf, permission to perform an assessment, audit, examination or review of all controls in the Contractor's physical and technical environment in relation to all Personal Information that is Used by the Contractor pursuant to this Agreement. The Contractor shall fully cooperate with such assessment, audit or examination, as applicable, by providing the County or the third party on the County's behalf, access to all Authorized Employees and other knowledgeable personnel, physical premises, documentation, infrastructure and application software that is Used by the Contractor for Personal Information pursuant to this Agreement. In addition, the Contractor shall provide the County with the results of any audit by or on behalf of the Contractor that assesses the effectiveness of the Contractor's information security program as relevant to the security and confidentiality of Personal Information Used by the Contractor or Authorized Persons during the course of this Agreement under this Exhibit E.
- (C) The Contractor shall ensure that all Authorized Persons who Use Personal Information agree to the same restrictions and conditions in this Exhibit E. that apply to the Contractor with respect to such Personal Information by incorporating the relevant provisions of these provisions into a valid and binding written agreement between the Contractor and such Authorized Persons, or amending any written agreements to provide same.

**6. Return or Destruction of Personal Information.** Upon the termination of this Agreement, the Contractor shall, and shall instruct all Authorized Persons to, promptly return to the County

## Exhibit E – Data Security

all Personal Information, whether in written, electronic or other form or media, in its possession or the possession of such Authorized Persons, in a machine readable form used by the County at the time of such return, or upon the express prior written consent of the Director, securely destroy all such Personal Information, and certify in writing to the County that such Personal Information have been returned to the County or disposed of securely, as applicable. If the Contractor is authorized to dispose of any such Personal Information, as provided in this Exhibit E, such certification shall state the date, time, and manner (including standard) of disposal and by whom, specifying the title of the individual. The Contractor shall comply with all reasonable directions provided by the Director with respect to the return or disposal of Personal Information and copies of Personal Information. If return or disposal of such Personal Information or copies of Personal Information is not feasible, the Contractor shall notify the County according, specifying the reason, and continue to extend the protections of this Exhibit E to all such Personal Information and copies of Personal Information. The Contractor shall not retain any copy of any Personal Information after returning or disposing of Personal Information as required by this section 6. The Contractor's obligations under this section 6 survive the termination of this Agreement and apply to all Personal Information that the Contractor retains if return or disposal is not feasible and to all Personal Information that the Contractor may later discover.

**7. Equitable Relief.** The Contractor acknowledges that any breach of its covenants or obligations set forth in this Exhibit E may cause the County irreparable harm for which monetary damages would not be adequate compensation and agrees that, in the event of such breach or threatened breach, the County is entitled to seek equitable relief, including a restraining order, injunctive relief, specific performance and any other relief that may be available from any court, in addition to any other remedy to which the County may be entitled at law or in equity. Such remedies shall not be deemed to be exclusive but shall be in addition to all other remedies available to the County at law or in equity or under this Agreement.

**8. Indemnity.** The Contractor shall defend, indemnify and hold harmless the County, its officers, employees, and agents, (each, a **"County Indemnitee"**) from and against any and all infringement of intellectual property including, but not limited to infringement of copyright, trademark, and trade dress, invasion of privacy, information theft, and extortion, unauthorized Use, Disclosure, or modification of, or any loss or destruction of, or any corruption of or damage to, Personal Information, Security Breach response and remedy costs, credit monitoring expenses, forfeitures, losses, damages, liabilities, deficiencies, actions, judgments, interest, awards, fines and penalties (including regulatory fines and penalties), costs or expenses of whatever kind, including attorneys' fees and costs, the cost of enforcing any right to indemnification or defense under this Exhibit E and the cost of pursuing any insurance providers, arising out of or resulting from any third party claim or action against any County Indemnitee in relation to the Contractor's, its officers, employees, or agents, or any Authorized Employee's or Authorized Person's, performance or failure to perform under this Exhibit E or arising out of or resulting from the Contractor's failure to comply with any of its obligations under this section 8. The provisions of this section 8 do not apply to the acts or omissions of the County. The provisions of this section 8 are cumulative to any other obligation of the Contractor

## Exhibit E – Data Security

to, defend, indemnify, or hold harmless any County Indemnitee under this Agreement. The provisions of this section 8 shall survive the termination of this Agreement.

**9. Survival.** The respective rights and obligations of the Contractor and the County as stated in this Exhibit E shall survive the termination of this Agreement.

**10. No Third Party Beneficiary.** Nothing express or implied in the provisions of in this Exhibit E is intended to confer, nor shall anything in this Exhibit E confer, upon any person other than the County or the Contractor and their respective successors or assignees, any rights, remedies, obligations or liabilities whatsoever.

**11. No County Warranty.** The County does not make any warranty or representation whether any Personal Information in the Contractor's (or any Authorized Person's) possession or control, or Use by the Contractor (or any Authorized Person), pursuant to the terms of this Agreement is or will be secure from unauthorized Use, or a Security Breach or Privacy Practices Complaint.

## Exhibit F – Technology Standards

### 3. Definitions

12.18 Capitalized terms used in this Exhibit F have the meanings set forth in this section 1.

- a. **“Agency Hosted”** means applications that are hosted by County.
- b. **“Authorized Persons”** means any and all of the Contractor’s employees, subcontractors, representatives, agents, outsourcers, consultants, and providers of professional services to the Contractor
- c. **“CJIS”** stands for Criminal Justice Information Systems
- d. **“CLETS”** means the California Law Enforcement Telecommunications System
- e. **“FSO”** means the Fresno County Sheriff’s Office.
- f. **“Lifecycle”** means the active life of the Product before a declaration of End of Life.
- g. **“NCIC”** stands for National Crime Information Center
- h. **“Product”** means the computer hardware, software, and services provided by Contractor.
- i. **“SaaS”** means ‘Software as a Service’ applications and infrastructure that are hosted by Contractor.
- j. **“SAML”** stands for Security Assertion Markup Language
- k. **“SLA”** stands for Service Level Agreement
- l. **“SSO”** stands for Single Sign-On

### 4. Information Technology Strategy

The overall IT strategy of the Fresno Sheriff’s Office includes managing systems that are expandable and serviceable by Sheriff’s Information Technology personnel. Sheriff’s IT personnel shall be able to maintain systems without affecting functionality and systems shall remain scalable and flexible to adapt efficiently to changes in public safety needs. Systems shall be capable of supporting evolving technology environments and government security compliance.

### 5. Contractor Requirements

- a. Contractor agrees to comply with the personnel background clearance required by the FSO for any Authorized Persons that will have access to data or facilities
- b. Contractor shall not access any FSO data without prior notification to and/or formal authorization from FSO. Any unauthorized access to the data by the Contractor will be

## **Exhibit F – Technology Standards**

considered a security breach and Contractor shall follow the Security Breach Procedures outlined in Section 4 of Exhibit E – Data Security.

### **6. Product Requirements**

In furtherance of the overall Information Technology Strategy, Contractor covenants, represents and warrants to the County that the Product shall:

- a. Be supported throughout its Lifecycle with untethered access to major components and the ability to make modifications as needed.
- b. Apply Agency Hosted or SaaS architecture only. If both are available from the Contractor, Sheriff's IT personnel will make the final determination on which system type is most appropriate at the time of deployment.
- c. Employ interface methods that support integration with existing legacy systems.
- d. Provide County technical staff full administrative access to all tables and configuration tools.
- e. Provide access to an API, when available, that may be used by County technical staff to build interfaces as well as interfacing with other external agencies or County service providers.
- f. Include a user interface for configuration of screens
- g. Utilize services that are compliant with CJIS Security Policy to ensure government and agency security and compliance requirements are met.
- h. Support a variety of modern web browsers, such as Google Chrome, Mozilla Firefox and Microsoft Edge
- i. Support client access through VPN connectivity or Microsoft Azure App Proxy
- j. Utilize dynamic scaling in anticipation of changes in usage or resource intensive temporary processes
- k. Interface with on-prem environment for CLETS and NCIC
- l. Comply with latest published FBI CJIS Security Policy (version 5.9.3 dated 9/14/2023 or later)
- m. Implement SSO using SAML 2.0 or OpenID Connect 1.0/OAuth 2.0
- n. Utilize role-based access control for users and User and Entity Based Behavioral Analytics (UEBA)
- o. Provide Self-service event logging for on demand user and security audits
- p. Allow FSO IT unrestricted access to export (including bulk export) data via self-service.

### **7. Agency Hosted systems**

## Exhibit F – Technology Standards

Contractor covenants, represents, and warrants to the County that its Agency Hosted architecture Product supports:

- a. The latest server and end-user operating systems
- b. Deployable runtimes through device management (e.g., SCCM/Intune/GPO)
- c. Access to all agency and configuration data
- d. Resilient deployment models to minimize downtime for updates and regular maintenance
- e. Centralized logging and audit systems
- f. Authentication through SAML/OIDC with support for multi-factor authentication when required and provide regular updates for deployed components.
- g. Deployment within a Kubernetes cluster, standard VMware vCenter environment or an industry standard IaaS solution.
- h. Functionality consistent with multiple data centers for redundancy, including potential cloud-based infrastructure, to minimize downtime.
- i. Use by multiple law enforcement agencies and share/restrict data access according to the source agency requirements.
- j. Interfacing with current and future FSO systems (to the extent disclosed prior to execution of this Agreement).
- k. Backup systems and processes that keep Product functional during the backup operation and generate data-consistent backup files while providing restore options down to the second for critical systems

### 8. SaaS systems

The Contractor covenants, represents and warrants to the County that its SaaS architecture Product:

- a. Includes support for serverless, infrastructure elasticity, infrastructure as code, micro services, containers, security, analytics, development practices specifically for cloud environments, continuous and portable deployments.
- b. Follows current industry standards and best practices for security, reliability, and operational efficiency
- c. Shall be hosted on infrastructure compliant with government and agency requirements (CJIS, etc.)
- d. Shall utilize encryption for data in transit and for data at rest, as well as provide event logging, on demand user audits, cloud threat detection services and software deployment and delivery management.



## Exhibit F – Technology Standards

- e. Hosted on infrastructure located within the Continental United States and with a provider approved for government use (i.e., Azure Government, AWS GovCloud, etc.)
  - f. Provides a SLA that supports 24/365 operational days for all cloud services used and overall composite SLA of the proposed application architecture to achieve 99.999% uptime
  - g. Employs Distributed Denial of Service (DDoS) protection and cloud threat detection with easy-to-read security logs and reports
  - h. Is compliant with FedRAMP Security Standards
9. **Survival.** The respective rights and obligations of the Contractor and the County as stated in this Exhibit F shall survive the termination of this Agreement.