SUBMITTAL TO THE BOARD OF SUPERVISORS
COUNTY OF RIVERSIDE, STATE OF CALIFORNIA

ITEM: 3.47
(ID # 30597)
MEETING DATE:
Tuesday, June 23, 2026

FROM : PUBLIC SOCIAL SERVICES

SUBJECT: DEPARTMENT OF PUBLIC SOCIAL SERVICES (DPSS): Approve the Professional Services Agreement DPSS-0005468 with JUMP Technology Services, LLC., for LEAPS Case Management System and Software Maintenance, a Software-as-a-Service, for Adult Protective Services (APS), without seeking competitive bids, for 5 years effective July 1, 2026 through June 30, 2031; [All Districts] [Total Aggregate Cost: $972,325 and up to $194,465 in additional compensation]; [48% Federal, 36% State, 16% Realignment]

RECOMMENDED MOTION: That the Board of Supervisors:

1. Approve the Professional Services Agreement DPSS-0005468 with JUMP Technology Services, LLC for LEAPS Case Management System and Software Maintenance, a Software-as-a-Service, for Adult Protective Services (APS), without seeking competitive bids, for a total aggregate amount of $972,325, for 5 years effective July 1, 2026 through June 30, 2031, and authorize the Chair of the Board to sign the Agreement on behalf of the County; and,

2. Authorize the Purchasing Agent to issue a Purchase Order(s) for any goods and/or services rendered; and,

3. Authorize the Purchasing Agent, in accordance with Ordinance No. 459, based on the availability of fiscal funding and as approved to form by County Counsel to (a) sign amendments that make modifications to the scope of services that stay within the intent of the Agreement, and (b) sign amendments to the compensation provisions that do not exceed the sum total of twenty percent (20%) of the total amount of the agreement.

ACTION:Policy

Charity Douglas, DPSS Director 6/8/2026

MINUTES OF THE BOARD OF SUPERVISORS

On motion of Supervisor Perez, seconded by Supervisor Gutierrez and duly carried by unanimous vote, IT WAS ORDERED that the above matter is approved as recommended.

Ayes:	Medina, Spiegel, Washington, Perez, and Gutierrez
Nays:	None
Absent:	None
Date:	June 23, 2026
xc:	DPSS

Kimberly A. Rector
Clerk of the Board
By: _____
Deputy

FINANCIAL DATA	Current Fiscal Year:	Next Fiscal Year:	Total Cost:	Ongoing Cost
COST	$ 0	$ 194,465	$ 972,325	$ 0
NET COUNTY COST	$ 0	$ 0	$ 0	$ 0

SOURCE OF FUNDS: 48% Federal, 36% State, 16% Realignment	**Budget Adjustment:** No
	For Fiscal Year: 26/27 – 30/31

C.E.O. RECOMMENDATION: Approve

BACKGROUND:

Summary

The Department of Public Social Services (DPSS) seeks Board approval to execute a five-year Professional Services Agreement (DPSS-0005468), procured through Sole Source Justification (26-203), with JUMP Technology Services, LLC, in the amount of $972,325, effective July 1, 2026 through June 30, 2031, for continued use and maintenance of the Adult Protective Services (APS) LEAPS Case Management System. JUMP offers expertise in devising innovative Health and Human Services solutions and provides a unique mix of prebuilt system modules that leverages the efficiency of custom APS software.

Since 2015, JUMP Technology Services has provided software maintenance and support for LEAPS, a cloud-based, Software-as-a-Service (SaaS) platform used by APS Social Workers to document and manage cases of elder and dependent adult abuse. LEAPS is currently utilized by 54 of California's 58 counties and offers unique features including:

- Cross-county case sharing for improved coordination and timely reporting.
- Access to historical data across jurisdictions, aiding service to transient and homeless populations.
- Family contact tracing across counties, exclusive to LEAPS.
- Mobile data capture for real-time, field-based case entry.
- 24/7/365 technical support from JUMP Technology Services.

The system also supports Riverside County's participation in the Home Safe program, enabling automated data collection and reporting in compliance with CDSS requirements under AB 1811. Due to the proprietary nature of LEAPS, only JUMP Technology Services is authorized and technically capable of performing system enhancements, modifications, and maintenance. Continued use of LEAPS ensures uninterrupted service delivery, compliance with state mandates, and alignment with departmental procedures.

Impact on Residents and Businesses

The LEAPS system provides APS with a comprehensive information management solution to

ensure the health and safety of elder and dependent adults throughout Riverside County. DPSS's APS unit is required to provide an in-person response, 24-hours a day, 7 days a week.

Additional Fiscal Information

The budget is as follows:

FISCAL YEAR PERIOD	SOFTWARE LICENSE (Level 300-400)	HOME SAFE DATA SUPPORT	ENHANCEMENTS	ANNUAL AMOUNT
July 1, 2026 through June 30, 2027	$155,015	$21,950	$17,500	$194,465
July 1, 2027 through June 30, 2028	$155,015	$21,950	$17,500	$194,465
July 1, 2028 through June 30, 2029	$155,015	$21,950	$17,500	$194,465
July 1, 2029 through June 30, 2030	$155,015	$21,950	$17,500	$194,465
July 1, 2030 through June 30, 2031	$155,015	$21,950	$17,500	$194,465
Maximum Reimbursable Amount:	**$775,075**	**$109,750**	**$87,500**	**$972,325**

Contract History and Price Reasonableness

JUMP Technology Services were competitively procured and awarded through Request for Quotation (RFQ) #DPARC-466 released on September 9, 2015. On December 29, 2015, DPSS entered into an agreement with JUMP Technology Services L.L.C. for the provision of Adult Protective Services (APS) Case Management Services.

DPSS entered into an agreement with JUMP Technology Services, L.L.C. through a sole source (518882321) on July 1, 2021 and the current agreement expires on June 30, 2026.

DPSS has worked closely with JUMP since 2015 to enhance the LEAPS system to ensure it meets the County's needs. The advantages of continuing with the LEAPS system significantly outweigh the costs, risks, and operational disruptions associated with transitioning to a new platform. LEAPS is implemented statewide across California and has been deemed compliant at the state level, further reinforcing its reliability and suitability for ongoing use.

Given these factors, issuing a Request for Proposals (RFP) for these services would not be an effective or practical approach. Approval of this agreement via SSJ#26-203 will ensure services continue uninterrupted.

ATTACHMENTS:

A. Professional Services Agreement DPSS-0005468 with JUMP Technology Services LLC., APS LEAPS Case Management Agreement
B. Sole Source Justification 26-203

Melissa Curtis
Melissa Curtis, Deputy Director of Purchasing and Fleet 6/11/2026

Stacey Pena
Stacey Pena, EO Management Analyst 6/16/2026

Gregg Gu
Gregg Gu, Chief Deputy County Counsel 6/12/2026

County of Riverside Department of Public Social Services
Contracts Administration Unit
4060 County Circle Drive
Riverside, CA 92503

and

JUMP Technology Services, L.L.C., an Oklahoma limited liability company
Adult Services LEAPS Case Management System
DPSS-0005468

TABLE OF CONTENTS

List of Schedules
Schedule A – Payment Provisions
Schedule B – Scope of Services

List of Attachments
Attachment I – HIPAA Business Associate Agreement
Attachment II – PII Privacy and Security Standards
Attachment III – Medi-Cal Privacy & Security Agreement
Attachment IV – DPSS 2076A, DPSS 2076B & Instructions
Attachment V - JUMP Technology Services, LLC Enterprise Subscription Agreement

This Agreement for Adult Services LEAPS Case Management System DPSS-0005468 (hereinafter the "Agreement" also referred to as "County Agreement") is made and entered into by and between JUMP Technology Services, L.L.C., an Oklahoma limited liability company (herein referred to as "CONTRACTOR"), and the County of Riverside, a political subdivision of the State of California, on behalf of its Department of Public Social Services (herein referred to as "COUNTY"). The JUMP Technology Services, LLC Enterprise Subscription Agreement (hereinafter "Subscription Agreement"), attached hereto as Attachment V, is entered into pursuant to and incorporated into the Agreement, and will become effective July 1, 2026, in accordance with its terms. If any term in the Subscription Agreement conflicts with this County Agreement, the County Agreement shall govern. The parties agree as follows:

1. DEFINITIONS

A. "Agreement" refers to the terms and conditions, schedules, and attachments included herein.

B. "Authorized Users" means a user that has been permitted to use the Licensed Software, Sublicensed Software, Services, and/or Platform as described in Attachment V, Enterprise Subscription Agreement (Order Form).

C. "Clarity" is the brand name of the HMIS software platform.

D. "CONTRACTOR" refers to JUMP Technology Services, L.L.C. including its employees, agents, representatives, subcontractors, and suppliers.

E. "COUNTY" refers to the County of Riverside.

F. "COUNTY Data" shall mean all electronic data or information submitted by COUNTY to the Licensed Software or Services but excluding Deidentified Data (as defined below).

G. "DPSS" or "COUNTY" refers to the County of Riverside's Department of Public Social Services, which has administrative responsibility for this Agreement.

H. "De-identified Data" refers to customer data that has been processed to remove or obscure all information that could reasonably identify an individual, and that has been independently certified by a compliant third party as suitable for the CONTRACTOR's use in analyzing operational performance.

I. "Help Desk Ticket (HDT)" refers to a problem identified by unique number in CONTRACTOR's Help Desk system.

J. "HMIS" refers to Homeless Management Information System.

K. "HHDRS" refers to Homeless Data Reporting Solution.

L. "Home Safe" refers to homeless prevention grant programs. The Home Safe Program was established by Assembly Bill (AB) 1811 to support the safety and housing stability of individuals involved in APS.

M. "HSAPS 19" refers to the Home Safe Adult Protective Services monthly status report.

N. "Enhancement" refers to any modification or addition that, when made or added to a software system, materially changes its utility, efficiency, functional capability, but that does not constitute solely an Error Correction. Enhancements may be designated by CONTRACTOR as minor or major, depending on CONTRACTOR's assessment of their value and of the function added to the software system.

O. “Error” refers to any failure of the software system to conform in all material responses to its functional specifications as documented in the software system manuals or scope of work.

P. “Error correction” refers to either a modification or an addition that, when made or added to a software system, establishes material conformity of the software system to the functional specifications or a procedure or routine that, when observed in the regular operation of the software system, eliminates the practical adverse effect on COUNTY of such nonconformity.

Q. “LEAPS” refers to JUMP Technology Services case management system.

R. “Licensed Software” shall mean the program specific Software as a Service to which the COUNTY is subscribing with individual licensed user accounts as set forth in Attachment V, Enterprise Subscription Agreement (Order Form).

S. “Order Form” means a work authorization executed by the Parties from time to time laying out the items being purchased by the COUNTY, scope of use, pricing, payment terms and any other relevant terms, which will be a part of and be governed by the terms and conditions of this County Agreement.

T. “Platform” shall mean the Software delivered under the Subscription Services which includes supporting software, and programming, and user interfaces to Authorized Users as set forth in Attachment V Enterprise Subscription Agreement (Order Form).

U. “Professional Services” means, collectively, the implementation, installation, data conversion, consultation, and training services provided by CONTRACTOR under or in connection with this Agreement.

V. “Services” shall mean the Professional Services and the Subscription Services set forth in Attachment V, Enterprise Subscription Agreement (Order Form).

W. “Software” means the object code version of computer programs developed by CONTRACTOR and listed on an Order Form, including Updates furnished to COUNTY by CONTRACTOR pursuant to this Agreement or any Order Form, but excluding all Sublicensed Software or third party software.

X. “SSC” refers to CONTRACTOR’s Technology Services Support Center.

Y. “Subcontract” refers to any contract, purchase order, or other purchase agreement, including modifications and change orders to the foregoing, entered into by the Contractor with a subcontractor to furnish supplies, materials, equipment, and services for the performance of any of the terms and conditions contained in this Agreement.

Z. “Subcontractor” refers to any supplier, vendor, or firm that furnishes supplies, materials, equipment, or services to or for the Contractor or another subcontractor.

AA. “Subscription Services” shall mean the services to keep the Licensed Software in working order and to sustain useful life of the Licensed Software, including Updates and specified in Attachment V, Enterprise Subscription Agreement (Order Form).

BB. “Statio Portal” shall mean a secure, California Department of Social Services (CDSS) online system used for Home Safe Program data entry, data correction, reporting and partner access.

CC. “Undertaking” refers to responsibility as referenced in CONTRACTOR’s Attachment V, Enterprise Subscription Agreement (Order Form).

2. DESCRIPTION OF SERVICES

CONTRACTOR shall provide all services at the prices stated in Schedule A, Payment Provisions, and as outlined and specified in Schedule B, Scope of Services, and Attachment I HIPAA Business Associate Agreement, Attachment II PII Privacy and Security Standards, Attachment III Medi-Cal Privacy & Security Agreement, Attachment IV DPSS 2076A, DPSS 2076B & Instructions and, Attachment V JUMP Technology Services, LLC Enterprise Subscription Agreement.

3. PERIOD OF PERFORMANCE

This Agreement shall be effective July 1, 2026 and continue through June 30, 2031, unless terminated earlier or otherwise modified. CONTRACTOR shall commence performance upon the effective date and shall diligently and continuously perform thereafter.

4. COMPENSATION

COUNTY shall pay CONTRACTOR for services performed, products provided, or expenses incurred in accordance with Schedule A, "Payment Provisions." COUNTY is not responsible for any fees or costs incurred above or beyond the contracted amount and shall have no obligation to purchase any specified amount of services or product. Unless otherwise specifically stated in Schedule A, COUNTY shall not be responsible for payment of any of CONTACTOR's expenses related to this Agreement. At the expiration of the term of this Agreement, or upon termination prior to the expiration of the Agreement, any funds paid to CONTRACTOR, but not used for purposes of this Agreement shall revert to COUNTY within thirty (30) calendar days of the expiration or termination.

5. AVAILABILITY OF FUNDS/NON-APPROPRIATION OF FUNDS

The obligation of COUNTY for payment under this Agreement beyond the current fiscal year is contingent upon and limited by the availability of county funding from which payment can be made. There shall be no legal liability for payment on the part of COUNTY beyond June 30 of each year unless funds are made available for such payment by the County Board of Supervisors. In the event such funds are not forthcoming for any reason, COUNTY shall immediately notify CONTRACTOR in writing and this Agreement shall be deemed terminated and be of no further force or effect. COUNTY shall make all payments to CONTRACTOR that were properly earned prior to the unavailability of funding.

6. TERMINATION

A. COUNTY may terminate this Agreement without cause upon giving thirty (30) calendar days written notice served on CONTRACTOR stating the extent and effective date of termination.

B. COUNTY may, upon five (5) calendar days written notice, terminate this Agreement for CONTRACTOR's default, if CONTRACTOR refuses or fails to comply with the terms of this Agreement, or fails to make progress that may endanger performance and does not immediately cure such failure. In the event of such termination, COUNTY may proceed with the work in any manner deemed proper by COUNTY.

C. After receipt of the notice of termination, CONTRACTOR shall:

(1) Stop all work under this Agreement on the date specified in the notice of termination; and

(2) Transfer to COUNTY and deliver in the manner directed by COUNTY any materials, reports or other products, which, if the Agreement had been completed or continued, would be required to be furnished to COUNTY.

D. After termination, COUNTY shall make payment only for CONTRACTOR's performance up to the date of termination in accordance with this Agreement.

E. CONTRACTOR's rights under this Agreement shall terminate (except for fees accrued prior to the date of termination) upon dishonestly or willful and material breach of this Agreement by CONTRACTOR; or in the event of CONTRACTOR's unwillingness or inability, for any reason whatsoever, to perform the terms of this Agreement. In such an event, CONTRACTOR shall not be entitled to any further compensation under this Agreement.

F. The rights and remedies of COUNTY provided in this section shall not be exclusive and are in addition to any other rights or remedies provided by law or this Agreement.

7. REQUEST FOR WAIVER AND WAIVER OF BREACH

Waiver of any provision of this Agreement must be in writing and signed by authorized representatives of the parties. No waiver or breach of any provision of the terms and conditions herein shall be deemed, for any purpose, to be a waiver or a breach of any other provision hereof, or of a continuing or subsequent waiver or breach. Failure of COUNTY to require exact, full compliance with any terms of this Agreement shall not be construed as making any changes to the terms of this Agreement and does not prevent COUNTY from enforcing the terms of this Agreement.

8. TRANSITION PERIOD

CONTRACTOR recognizes that the services under this Agreement are vital to COUNTY and must be continued without interruption and that, upon expiration, COUNTY or another contractor may continue the services outlined herein. CONTRACTOR agrees to exercise its best efforts and cooperation to effect an orderly and efficient transition of clients or services to a successor.

9. OWNERSHIP, PUBLICATION, REPRODUCTION, AND USE OF MATERIAL

COUNTY shall own all right, title, and interest in and to the COUNTY Data. CONTRACTOR shall own and retain all right, title, and interest in and to (i) each Platform, Software and the Services and all improvements, enhancements, test scripts, documents, or modifications thereto, (ii) any software, applications, inventions, or other technology developed in connection with the Services, and (iii) all intellectual property and proprietary rights in and related to any of the foregoing. CONTRACTOR shall grant to COUNTY a non-exclusive, non-transferable license to use the Platform only for COUNTY's own internal purposes in connection with the Licensed Software and Services.

10. DISPOSITION OF DATA

Upon request by COUNTY made before or within ninety (90) days after the effective date of termination, CONTRACTOR will make available to the COUNTY a complete and secure (i.e., encrypted and appropriately authenticated) download file of COUNTY Data including all available documentation in their native format PostgreSQL and/or delimited text files (e.g Microsoft SQL Server).

After providing the COUNTY at its request a copy of all COUNTY data or no later than ninety (90) days after the effective date of termination (whichever is later), CONTRACTOR shall destroy all COUNTY data in its possession.

11. CONDUCT OF CONTRACTOR/ CONFLICT OF INTEREST

A. CONTRACTOR covenants that it presently has no interest, including but not limited to, other projects or contract, and shall not acquire any such interest, direct or indirect, which would conflict in any manner or degree with CONTRACTOR's performance under this Agreement. CONTRACTOR further covenants that no person or subcontractor having any such interest shall be employed or retained by CONTRACTOR under this Agreement. CONTRACTOR agrees to inform the COUNTY of all CONTRACTOR's interest, if any, which are or may be perceived as incompatible with COUNTY's interests.

B. CONTRACTOR shall not, under any circumstances which could be perceived as an to influence the recipient in the conduct or his/her duties, accept any gratuity or special favor from individuals

or firms with whom CONTRACTOR is doing business or proposing to do business, in fulfilling this Agreement.

12. RECORDS, INSPECTIONS, AND AUDITS

A. All performance, including services, workmanship, materials, facilities or equipment utilized in the performance of this Agreement, shall be subject to inspection and test by COUNTY or any other regulatory agencies at all times. This may include, but is not limited to, monitoring or inspecting contractor performance through any combination of on-site visits, inspections, evaluations, and CONTRACTOR self-monitoring. CONTRACTOR shall cooperate with any inspector or COUNTY representative reviewing compliance with this Agreement and permit access to all necessary locations, equipment, materials, or other requested items.

B. CONTRACTOR shall maintain auditable books, records, documents, and other evidence relating to costs and expenses to this Agreement. CONTRACTOR shall maintain these records for at least three (3) years after final payment has been made or until pending county, state, and federal audits are completed, whichever is later.

C. Any authorized county, state or the federal representative shall have access to all books, documents, papers, electronic data and other records they determine are necessary to perform an audit, evaluation, inspection, review, assessment, or examination. These representatives are authorized to obtain excerpts, transcripts and copies as they deem necessary and shall have the same right to monitor or inspect the work or services as COUNTY.

D. If CONTRACTOR disagrees with an audit, CONTRACTOR may employ a Certified Public Accountant (CPA) to prepare and file with COUNTY its own certified financial and compliance audit. CONTRACTOR shall not be reimbursed by COUNTY for such an audit regardless of the audit outcome.

E. CONTRACTOR shall establish sufficient procedures to self-monitor the quality of services/products under this Agreement and shall permit COUNTY or other inspector to assess and evaluate CONTRACTOR's performance at any time, upon reasonable notice to the CONTRACTOR.

13. CONFIDENTIALITY

A. As required by applicable law, COUNTY and CONTRACTOR shall maintain the privacy and confidentiality of all information and records, regardless of format, received pursuant to the Agreement ("confidential information"). Confidential information includes, but is not limited to, unpublished or sensitive technological or scientific information; medical, personnel, or security records; material requirements or pricing/purchasing actions; COUNTY information or data which is not subject to public disclosure; COUNTY operational procedures; and knowledge of contractors, subcontractors or suppliers in advance of official announcement. CONTRACTOR shall ensure that no person will publish, disclose, use or cause to be disclosed such confidential information pertaining to any applicant or recipient of services. CONTRACTOR shall keep all confidential information received from COUNTY in the strictest confidence. CONTRACTOR shall comply with Welfare and Institutions Code Section 10850.

B. CONTRACTOR shall take special precautions, including but not limited to, sufficient training of CONTRACTOR's staff before they begin work, to protect such confidential information from loss or unauthorized use, access, disclosure, modification or destruction.

C. CONTRACTOR shall ensure case record or personal information is kept confidential when it identifies an individual by name, address, or other specific information. CONTRACTOR shall not use such information for any purpose other than carrying out CONTRACTOR's obligations under this Agreement.

D. CONTRACTOR shall promptly transmit to COUNTY all third party requests for disclosure of confidential information. CONTRACTOR shall not disclose such information to anyone other than COUNTY except when disclosure is specifically permitted by this Agreement or as authorized in writing in advance by COUNTY.

14. HEALTH INSURANCE PORTABILITY ACCOUNTABILITY ACT

CONTRACTOR is subject to and shall operate in compliance with all relevant requirements contained in the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191, enacted August 21, 1996, and the related laws and regulations promulgated subsequent thereto. The parties agree to the terms and conditions the HIPAA Business Associated attached as Attachment I.

15. PERSONALLY IDENTIFIABLE INFORMATION

A. Personally Identifiable Information (PII) refers to personally identifiable information that can be used alone or in conjunction with any other reasonably available information, to identify a specific individual. PII includes, but is not limited to, an individual's name, social security number, driver's license number, identification number, biometric records, date of birth, place of birth, or mother's maiden name. The PII may be electronic, paper, verbal, or recorded. PII may collected performing administrative functions on behalf of programs, such as determining eligibility for, or enrollment in, and collecting PII for such purposes, to the extent such activities are authorized by law.

B. CONTRACTOR may use or disclose PII only to perform functions, activities or services directly related to the administration of programs in accordance with Welfare and Institutions Code sections 10850 and 14100.2, or 42 Code of Federal Regulations (CFR) section 431.300 et.seq, and 45 CFR 205.50 et.seq, or as required by law. Disclosures which are required by law, such as a court order, or which are made with the explicit written authorization of the client, are allowable. Any other use or disclosure of requires the express approval in writing of the COUNTY. CONTRACTOR shall not duplicate, disseminate or disclose PII except as allowed in this Agreement.

C. CONTRACTOR agrees to the PII Privacy and Security Standards attached as Attachment II. When applicable, CONTRACTOR shall incorporate the relevant provisions of Attachment II into each subcontract or sub-award to subcontractors.

16. MEDI-CAL PERSONALLY IDENTIFIABLE INFORMATION

"Medi-Cal PII" refers to Medi-Cal Personally Identifiable Information which is directly obtained in the course of performing an administrative function on behalf of Medi-Cal, such as determining Medi-Cal eligibility or conducting In Home Supportive Services (IHSS) operations, that can be used alone, or in conjunction with any other information, to identify a specific individual. PII includes any information that can be used to search for or identify individuals, or can be used to access their files, such as name, social security number, date of birth, driver's license number or identification number. PII may be electronic or paper.

The CONTRACTOR may use or disclose Medi-Cal Personally Identifiable Information (PII) only to perform functions, activities or services directly related to the administration of the Medi-Cal program in accordance with Welfare and Institutions Code section 14100.2 and 42 Code of Federal Regulations section 431.300 et.seq, or as required by law. Disclosures which are required by law, such as a court order, or which are made with the explicit written authorization of the Medi-Cal client, are allowable. Any other use or disclosure of Medi-Cal PII requires the express approval in writing of the COUNTY. The CONTRACTOR shall not duplicate, disseminate or disclose Medi-Cal PII except as allowed in this Agreement.

The CONTRACTOR agrees to the same privacy and security safeguards as are contained in the Medi-Cal Data Privacy and Security Agreement, attached hereto and incorporated by this reference as Attachment III.

When applicable, the CONTRACTOR shall incorporate the relevant provisions of Attachment III into each subcontract or sub-award to subcontractors.

17. HOLD HARMLESS/INDEMNIFICATION

CONTRACTOR agrees to indemnify and hold harmless COUNTY, its departments, agencies and districts, including their officers, employees and agents (collectively "County Indemnitees"), from any liability, damage, claim or action based upon or related to any services or work of CONTRACTOR (including its officers, employees, agents, subcontractors or suppliers) arising out of or in any way relating to this Agreement, including but not limited to property damage, bodily injury or death. CONTRACTOR shall, at its sole expense and cost including but not limited to, attorney fees, cost of investigation, defense, and settlements or awards, defend County Indemnitees in any such claim or action. CONTRACTOR shall, at their sole cost, have the right to use counsel of their choice, subject to the approval of COUNTY which shall not be unreasonably withheld; and shall have the right to adjust, settle, or compromise any such claim or action so long as that does not compromise CONTRACTOR's indemnification obligation. CONTRACTOR's obligation hereunder shall be satisfied when CONTRACTOR has provided COUNTY the appropriate form of dismissal relieving COUNTY from any liability for the action or claim made. The insurance requirements stated in this Agreement shall in no way limit or circumscribe CONTRACTOR's obligations to indemnify and hold COUNTY harmless.

18. INSURANCE

A. Without limiting or diminishing the CONTRACTOR'S obligation to indemnify or hold the COUNTY harmless, CONTRACTOR shall procure and maintain or cause to be maintained, at its sole cost and expense, the following insurance coverage's during the term of this Agreement. As respects to the insurance section only, the COUNTY herein refers to the County of Riverside, its Agencies, Districts, Special Districts, and Departments, their respective directors, officers, Board of Supervisors, employees, elected or appointed officials, agents or representatives as Additional Insureds.

B. Any insurance carrier providing insurance coverage hereunder shall be admitted to the State of California and have an AM BEST rating of not less than A: VIII (A:8) unless such requirements are waived, in writing, by the County Risk Manager. If the County's Risk Manager waives a requirement for a particular insurer such waiver is only valid for that specific insurer and only for one policy term.

C. CONTRACTOR's insurance carrier(s) must declare its insurance self-insured retentions. If such self-insured retentions exceed $500,000 per occurrence such retentions shall have the prior written consent of the County Risk Manager before the commencement of operations under this Agreement. Upon notification of self-insured retention unacceptable to COUNTY, and at the election of the County's Risk Manager, CONTRACTOR's carriers shall either; 1) reduce or eliminate such self-insured retention as respects to this Agreement with COUNTY, or 2) procure a bond which guarantees payment of losses and related investigations, claims administration, and defense costs and expenses.

D. CONTRACTOR shall cause CONTRACTOR's insurance carrier(s) to furnish the COUNTY with either 1) a properly executed original certificate(s) of insurance and certified original copies of endorsements effecting coverage as required herein, or 2) if requested to do so orally or in writing by the County Risk Manager, provide original certified copies of policies, including all endorsements and all attachments thereto, showing such insurance is in full force and effect. Further, said Certificate(s) and policies of insurance shall contain the covenant of the insurance

carrier(s) that thirty (30) calendar days written notice shall be given to the COUNTY prior to any material modification, cancellation, expiration or reduction in coverage of such insurance. In the event of a material modification, cancellation, expiration, or reduction in coverage, this Agreement shall terminate forthwith, unless the COUNTY receives, prior to such effective date, another properly executed original Certificate of Insurance and original copies of endorsements or certified original policies, including all endorsements and attachments thereto evidencing coverages set forth herein and the insurance required herein is in full force and effect. CONTRACTOR shall not commence operations until the COUNTY has been furnished original certificate(s) of insurance and certified original copies of endorsements and if requested, certified original policies of insurance including all endorsements and any and all other attachments as required in this section. An individual authorized by the insurance carrier to do so on its behalf shall sign the original endorsements for each policy and the certificate of insurance.

E. It is understood and agreed to by the parties hereto that CONTRACTOR's insurance shall be construed as primary insurance, and COUNTY's insurance and/or deductibles and/or self-insured retentions or self-insured programs shall not be construed as contributory.

F. If, during the term of this Agreement or any extension thereof, there is a material change in the scope of services, or there is a material change in the equipment to be used in the performance of the scope of work which will add additional exposures (such as the use of aircraft, watercraft, cranes, etc.), or the term of this Agreement, including any extensions thereof, exceeds five (5) years, the COUNTY reserves the right to adjust the types of insurance required under this Agreement and the monetary limits of liability for the insurance coverages currently required herein if, in the County Risk Manager's reasonable judgment, the amount or type of insurance carried by the CONTRACTOR has become inadequate.

G. CONTRACTOR shall pass down the insurance obligations contained herein to all tiers of subcontractors working under this Agreement.

H. The insurance requirements contained in this Agreement may be met with a program(s) of self-insurance acceptable to COUNTY.

I. CONTRACTOR agrees to notify COUNTY of any claim by a third party or any incident or event that may give rise to a claim arising from the performance of this Agreement.

J. If CONTRACTOR maintains broader coverage and/or higher limits than the minimums shown below, COUNTY requires and shall be entitled to the broader coverage and/or higher limits maintained by CONTRACTOR. Any available insurance proceeds in excess of the specified minimum limits of insurance and coverage shall be available to COUNTY.

19. WORKER'S COMPENSATION

If the CONTRACTOR has employees as defined by the State of California, the CONTRACTOR shall maintain statutory Workers' Compensation Insurance (Coverage A) as prescribed by the laws of the State of California. Policy shall include Employers' Liability (Coverage B) including Occupational Disease with limits not less than $1,000,000 per person per accident. The policy shall be endorsed to waive subrogation in favor of The County of Riverside. Policy shall name the COUNTY as Additional Insureds.

20. VEHICLE LIABILITY

If vehicles or mobile equipment are used in the performance of the obligations under this Agreement, then CONTRACTOR shall maintain liability insurance for all owned, non-owned or hired vehicles so used in an amount not less than $1,000,000 per occurrence combined single limit. If such insurance contains a general aggregate limit, it shall apply separately to this agreement or be no less than two (2) times the occurrence limit. Policy shall name the COUNTY as Additional Insureds.

21. COMMERCIAL GENERAL LIABILITY

Commercial General Liability insurance coverage, including but not limited to, premises liability, unmodified contractual liability, products and completed operations liability, personal and advertising injury, and cross liability coverage, covering claims which may arise from or out of CONTRACTOR'S performance of its obligations hereunder. Policy shall name the COUNTY as Additional Insured. Policy's limit of liability shall not be less than $2,000,000 per occurrence combined single limit. If such insurance contains a general aggregate limit, it shall apply separately to this agreement or be no less than two (2) times the occurrence limit.

Policy shall include abuse and molestation insurance as an endorsement to the commercial general liability policy in a form and with coverage that are satisfactory to the County covering damages arising out of actual, threatened or allege physical abuse, mental injury, sexual molestation, negligent: hiring, employment, supervision, investigation, reporting or failure to report to proper authorities, a person(s) who committed any act of abuse, molestation, harassment, mistreatment or maltreatment of sexual nature and retention of any person for whom the contractor is responsible including but not limited to contractor and contractor's employees and volunteers. Policy endorsement's definition of an insured shall include the contractor, and the contractor's employees and volunteers. Coverage shall be written on an occurrence basis in an amount of not less than $2,000,000 per occurrence. If such insurance contains a general aggregate limit, it shall apply separately to this Agreement or be no less than two (2) times the occurrence limit. These limits shall be exclusive to this required coverage. Incidents related to or arising out of physical abuse, mental injury, or sexual molestation, whether committed by one or more individuals, and irrespective of the number of incidents or injuries or the time period or area over which the incidents or injuries occur, shall be treated as a separate occurrence for each victim. Coverage shall include the cost of defense, and the cost of defense shall be provided outside the coverage limit

22. CYBER LIABILITY

CONTRACTOR shall procure and maintain for the duration of the contract insurance against claims for injuries to person or damages to property which may arise from or in connection with the performance of the work hereunder by CONTRACTOR, its agents, representatives, or employees. CONTRACTOR shall procure and maintain for the duration of the contract insurance claims arising out of their services and including, but not limited to loss, damage, theft or other misuse of data, infringement of intellectual property, invasion of privacy and breach of data.

CONTRACTOR shall procure and maintain cyber liability Insurance, with limits not less than $2,000,000 per occurrence or claim, $2,000,000 aggregate. Coverage shall be sufficiently broad to respond to the duties and obligations as is undertaken by CONTRACTOR in this Agreement and shall include, but not limited to, claims involving infringement of intellectual property, including but not limited to infringement of copyright, trademark, trade dress, invasion of privacy violations, information theft, damage to or destruction of electronic information, release of private information, alteration of electronic information, extortion and network security. The policy shall provide coverage for breach response costs as well as regulatory fines and penalties as well as credit monitoring expenses with limits sufficient to respond to these obligations.

23. EXCESS/UMBRELLA LIABILITY INSURANCE

If any Excess or Umbrella Liability policies are used to meet the limits of liability required by this agreement, then said policies shall be "following form" of the underlying policy coverage, terms, conditions, and provisions and shall meet all of the insurance requirements stated in this document, including, but not limited to, the additional insured, contractual liability & "insured contract" definition for indemnity, occurrence, no limitation of prior work coverage, and primary & non-contributory insurance requirements stated therein. No insurance policies maintained by the Additional Insureds, whether primary or excess, and which also apply to a loss covered hereunder, shall be called upon to contribute to a loss until the Contractor's primary and excess liability policies are exhausted.

24. INDEPENDENT CONTRACTOR
It is agreed that CONTRACTOR is an independent contractor, and that no relationship of employer-employee exists between the parties. CONTRACTOR and its employees shall not be entitled to any benefits payable to employees of COUNTY, including but not limited to, workers' compensation, retirement, or health benefits. CONTRACTOR and its employees shall have no claim against COUNTY hereunder or otherwise for vacation pay, sick leave, retirement benefits, social security, worker's compensation, health or disability benefits, unemployment insurance benefits, or employee benefits of any kind. COUNTY shall not be required to make any deductions for CONTRACTOR employees from the compensation payable to CONTRACTOR under this Agreement. CONTRACTOR agrees to hold COUNTY harmless from any and all claims that may be made against COUNTY based upon any contention by any person or other party that an employer-employee relationship exists by reason of this Agreement. CONTRACTOR agrees to indemnify and defend, at its sole expense and cost, including but not limited, to attorney fees, cost of investigation, defense and settlements, or awards, COUNTY, its officers, agents, and employees in any legal action based upon such alleged existence of an employer-employee relationship by reason of this Agreement.

25. USE BY POLITICAL ENTITIES
CONTRACTOR agrees to extend the same pricing, terms, and conditions as stated in this Agreement to each and every political entity, special district, and related non-profit entity in Riverside County, and to every political entity located in the State of California. It is understood that other entities shall make purchases in their own name, make direct payment, and be liable directly to CONTRACTOR; and COUNTY shall in no way be responsible to CONTRACTOR for other entities' purchases.

26. LICENSES AND PERMITS
If applicable, CONTRACTOR shall be licensed and have all permits as required by Federal, State, County, or other regulatory authorities at the time the proposal is submitted to COUNTY and throughout the term of this Agreement. CONTRACTOR warrants that it has all necessary permits, approvals, certificates, waivers, and exceptions necessary for performance of this Agreement.

27. NO DEBARMENT OR SUSPENSION
CONTRACTOR certifies that it is not presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from covered transactions by a federal department or agency; has not within a three-year period preceding this Agreement been convicted of or had a civil judgment rendered against it for the commission of fraud or a criminal offense in connection with obtaining, attempting to obtain, or performing a public (federal, state or local) transaction; violation of federal or state anti-trust status; commission of embezzlement, theft, forgery, bribery, falsification or destruction of records, making false statements, or receiving stolen property; is not presently indicted or otherwise criminally or civilly charged by a government entity (federal, state or local) with commission of any of the offenses enumerated herein; and has not within a three-year period preceding this Agreement had one or more public transactions (federal, state or local) terminated for cause or default.

28. COMPLIANCE WITH RULES, REGULATIONS, AND DIRECTIVES
CONTRACTOR shall comply with all rules, regulations, requirements and directives of the California Department of Social Services, other applicable State or Federal agencies, funding sources and other governing regulatory authorities which impose duties and regulations upon COUNTY related to this Agreement. These shall be equally applicable to and binding upon CONTRACTOR to the same extent as they are upon COUNTY.

29. LOBBYING
A. CONTRACTOR shall ensure no federal appropriated funds have been paid or will be paid by or on behalf of the undersigned, to any person for influencing or attempting to influence an officer or employee of any agency, a member of Congress, an officer or employee of Congress, or an

employee of a member of Congress in connection with the awarding of any federal contract, continuation, renewal, amendment, or modification of any federal contract, grant loan or cooperative agreement.

B. If any funds other than federal appropriated funds have been paid or will be paid to any person for influencing or attempting to influence an officer or employee of any agency, a member of Congress, an officer or employee of Congress, or an employee of a member of Congress in connection with such federal contract, grant, loan, or cooperative agreement, CONTRACTOR shall complete and submit Standard Form LLL, "Disclosure Form to Report Lobbying," in accordance with its instructions.

C. CONTRACTOR shall require that the language of this certification be included in the award document for sub-awards at all tiers, including subcontracts, sub-grants, and contract under grants, loans, and cooperative agreements, and that all sub-recipients shall certify and disclose accordingly.

30. ADVERSE GOVERNMENT ACTION

In the event any action of any department, branch or bureau of the federal, state, or local government has a material adverse effect on either party in the performance of their obligations hereunder, then that party shall notify the other of the nature of this action, including in the notice a copy of the adverse action. The parties shall meet within thirty (30) calendar days and shall, in good faith, attempt to negotiate a modification to this Agreement that minimizes the adverse effect. Notwithstanding the provisions herein, if the parties fail to reach a negotiated modification concerning the adverse action, then the affected party may terminate this Agreement by giving at least one hundred eighty (180) calendar days' notice or may terminate sooner if agreed to by both parties.

31. SUBCONTRACTS

A. CONTRACTOR shall not enter into any subcontract with any subcontractor who:

(1) Is presently debarred, suspended, proposed for debarment or suspension, or declared ineligible or voluntarily excluded from covered transactions by a federal department or agency;

(2) Has within a three-year period preceding this Agreement been convicted of or had a civil judgment rendered against them for the commission of fraud, a criminal offense in connection with obtaining, attempting to obtain, or performing a public (federal, state or local) transaction, violation of federal or state anti-trust status, commission of embezzlement, theft, forgery, bribery, falsification or destruction of records, making false statements, or receiving stolen property;

(3) Is presently indicted or otherwise criminally or civilly charged by a government entity (federal, state or local) with commission of any of the offenses enumerated in the paragraph above; and

(4) Has within a three-year period preceding this Agreement had one or more public transactions (federal, state or local) terminated for cause or default.

B. CONTRACTOR shall be fully responsible for the acts or omissions of its subcontractors and the subcontractors' employees.

C. CONTRACTOR shall insert clauses in all subcontracts to bind its subcontractors to the terms and conditions of this Agreement.

D. Nothing contained in this Agreement shall create a contractual relationship between any subcontractor or supplier of CONTRACTOR and COUNTY.

32. NO OFFSHORE WORK OR SERVICES
CONTRACTOR, its employees, agents, and/or subcontractors shall not: (i) perform any work, services, and/or obligations under this Master Agreement at any location outside of the United States of America (USA); and/or (ii) transmit COUNTY information related to this Master Agreement (including, but not limited to, public social services information, personally identifiable information, and/or protected health information (PHI) of the COUNTY) outside of the USA. Additionally, no CONTRACTOR employee, agents, and/or subcontractors outside of the USA will receive, process, transfer, handle, store or have access to COUNTY information in oral, written, or electronic form.

33. SUPPLANTATION
CONTRACTOR shall not supplant any federal, state or county funds intended for the purpose of this Agreement with any funds made available under any other agreement. CONTRACTOR shall not claim reimbursement from COUNTY for any sums which have been paid by another source of revenue. CONTRACTOR agrees that it will not use funds received pursuant to this Agreement, either directly or indirectly, as a contribution or compensation for purposes of obtaining state funds under any state program or COUNTY funds under any county programs without prior approval of COUNTY.

34. ASSIGNMENT
CONTRACTOR shall not assign or transfer any interest in this Agreement without the prior written consent of COUNTY. Any attempt to assign or transfer any interest without written consent of COUNTY shall be deemed void and of no force or effect.

35. FORCE MAJEURE
If either party is unable to comply with any provision of this Agreement due to causes beyond its reasonable control and which could not have been reasonably anticipated, such as acts of God, acts of war, civil disorders, or other similar acts, such party shall not be held liable for such failure to comply.

36. GOVERNING LAW
This Agreement shall be governed by the laws of the State of California. Any legal action related to the interpretation or performance of this Agreement shall be filed only in the Superior Court for the State of California or the U.S. District Court located in Riverside, California.

37. DISPUTES
A. The parties shall attempt to resolve any disputes amicably at the working level. If that is not successful, the dispute shall be referred to the senior management of the parties. Any dispute relating to this Agreement which is not resolved by the parties shall be decided by COUNTY's Compliance Contract Officer who shall furnish the decision in writing. The decision of COUNTY's Compliance Contract Officer shall be final and conclusive unless determined by a court to have been fraudulent, capricious, arbitrary, or so grossly erroneous as necessarily to imply bad faith. CONTRACTOR shall proceed diligently with the performance of this Agreement pending resolution of a dispute.

B. Prior to the filing of any legal action related to this Agreement, the parties shall be obligated to attend a mediation session in Riverside County before a neutral third party mediator. A second mediation session shall be required if the first session is not successful. The parties shall share the cost of the mediations.

38. ADMINISTRATIVE/CONTRACT LIAISON
Each party shall designate a liaison that will be the primary point of contact regarding this Agreement.

39. NOTICES

All notices, claims, correspondence, or statements authorized or required by this Agreement shall be deemed effective three (3) business days after they are made in writing and deposited in the United States mail addressed as follows:

COUNTY:
Department of Public Social Services
Contracts Administration Unit
P.O. Box 7789
Riverside, CA 92513

Invoices and other financial documents:
Department of Public Social Services
Fiscal/Management Reporting Unit
4060 County Circle Drive
Riverside, CA 92503
OperatingServicesContractPayments@rivco.org

CONTRACTOR:
JUMP Technology Services, L.L.C.
1201 Covell Village Dr. #436
Edmond, OK 73003

CONTRACTOR "Remit To" address:
JUMP Technology Services, L.L.C.
P.O. Box 3452
Edmond, OK 473083

40. SIGNED IN COUNTERPARTS

This agreement may be executed in any number of counterparts, each of which when executed shall constitute a duplicate original, but all counterparts together shall constitute a single agreement.

41. ELECTRONIC SIGNATURES

Each party of this Agreement agrees to the use of electronic signatures, such as digital signatures that meet the requirements of the California Uniform Electronic Transactions Act (("CUETA") Cal. Civ. Code §§ 1633.1 to 1633.17), for executing this Agreement. The parties further agree that the electronic signature(s) included herein are intended to authenticate this writing and to have the same force and effect as manual signatures. Electronic signature means an electronic sound, symbol, or process attached to or logically associated with an electronic record and executed or adopted by a person with the intent to sign the electronic record pursuant to the CUETA as amended from time to time. Digital signature means an electronic identifier, created by computer, intended by the party using it to have the same force and effect as the use of a manual signature, and shall be reasonably relied upon by the parties. For purposes of this section, a digital signature is a type of "electronic signature" as defined in subdivision (i) of Section 1633.2 of the Civil Code.

42. MODIFICATION OF TERMS

This Agreement may be modified only by a written amendment signed by authorized representatives of both parties. Requests to modify fiscal provisions shall be submitted no later than April 1.

43. ENTIRE AGREEMENT

This Agreement constitutes the entire agreement between the parties with respect to the subject matter hereof. All prior or contemporaneous agreements of any kind or nature relating to the same subject matter shall be of no force or effect.

Authorized Signature for JUMP Technology Services, L.L.C., an Oklahoma limited liability company Denise Brinkmeyer	Authorized Signature for County of Riverside, a political subdivision of the state of California on behalf of its Department of Public Social Services Karen S. Spiegel
Printed Name of Person Signing: Denise Brinkmeyer	Printed Name of Person Signing: Karen Spiegel
Title: President	Title: Chair of the Board
Date Signed: 06/05/2026	Date Signed: 06/23/2026

ATTEST:
Clerk of the Board
By: Whitney Mayo, Deputy

Approved as to Form
Minh C. Tran
County Counsel
Esen Sainz
Esen Sainz
Deputy County Counsel
Date: 06/05/2026

A.1 MAXIMUM AMOUNTS –ANNUAL AND AGGREGATE TOTALS

The total Maximum Reimbursable Amount (MRA) for this contract over a five-year period is $972,325, inclusive of all associated expenses. Within the scope of the agreement, funds may be reallocated between the Software License and the Maintenance and Support categories as needed, provided that the total aggregate amount of the contract is not exceeded. Any proposed reallocation of funds between these categories must receive advance written approval from the DPSS prior to implementation.

FISCAL YEAR PERIOD	SUBSCRIPTION SERVICES (Level 300-400)	HOME SAFE DATA SUPPORT	ENHANCEMENTS/ MAINTENANCE & SUPPORT (outside of Subscription Services	ANNUAL AMOUNT
July 1, 2026 through June 30, 2027	$155,015	$21,950	$17,500	$194,465
July 1, 2027 through June 30, 2028	$155,015	$21,950	$17,500	$194,465
July 1, 2028 through June 30, 2029	$155,015	$21,950	$17,500	$194,465
July 1, 2029 through June 30, 2030	$155,015	$21,950	$17,500	$194,465
July 1, 2030 through June 30, 2031	$155,015	$21,950	$17,500	$194,465
Maximum Reimbursable Amount:	$775,075	$109,750	$87,500	$972,325

1. A discretionary fund in the amount of $17,500 has been allocated for the full term of the agreement to cover costs that exceed (sixty) 60 credits.

2. Subscription Services – Licensing and Hosting of the LEAPS System for 300 to 400 users. Services include 60 Service Credits at no additional charge for COUNTY representatives to request one time services not included in licensing and hosting. Subscription Services also include weekly database backups made available to the COUNTY.

3. Home Safe Data Support - Maintenance of Home Safe Assessments and manage the Statio portal for data corrections and partner-program sharing capability. Export HSAPS-19 and HMIS data, including downloading HMIS data sets from Clarity and importing them into HHDRS. Provide ticket-system support for the product module and develop and maintain training materials.

4. Enhancements, Maintenance & Support – COUNTY may request one time professional services not included in licensing and hosting. JUMP will provide a quote for the service(s) along with a request for approval. Completed services will be invoiced. Services provided will conform to performance defined in V.

A.2 METHOD, TIME, AND CONDITIONS OF PAYMENT

A. CONTRACTOR shall be paid the actual amount of each approved invoice. COUNTY may delay payment if the required supporting documentation is not provided, or other requirements are not met. All complete claims submitted in a timely manner shall be processed within forty-five (45) calendar days.

B. As applicable for payment requests, CONTRACTOR shall submit completed DPSS Forms 2076A, 2076B (Attachment IV).

C. IF CONTRACTOR expends a combined annual total of $1,000,000 in federal funds, CONTRACTOR shall ensure that an independent fiscal audit is done annually. In the event that an audit is conducted, CONTRACTOR shall immediately provide a copy of the audit to COUNTY.

A.3 CONSUMER PRICE INDEX

No price increases will be permitted during the first year of this Agreement. All price decreases (for example, if CONTRACTOR offers lower prices to another governmental entity) will automatically be extended to COUNTY. COUNTY requires written proof satisfactory to COUNTY of cost increases prior to any approved price adjustment. After the first year of the award, a minimum of 30-days advance notice in writing is required to secure such adjustment. No retroactive price adjustments will be considered. Any price increases must be stated in a written amendment to this Agreement. The net dollar amount of profit will remain firm during the period of this Agreement. Annual increases shall not exceed the Consumer Price Index (CPI) for all consumers, all items for the Los Angeles, Riverside and Orange Counties CA areas and be subject to satisfactory performance review by COUNTY and approved (if needed) for budget funding by the Board of Supervisors.

A.4 FINANCIAL RESOURCES

During the term of this Agreement, CONTRACTOR shall maintain sufficient financial resources necessary to fully perform its obligations. CONTRACTOR confirms there has been no material financial change in CONTRACTOR (including any parent company) since its last financial statement that has resulted in a negative impact to its financial condition.

A.5 DISALLOWANCE

If CONTRACTOR receives payment under this Agreement which is later disallowed by COUNTY for nonconformance with the Agreement, CONTRACTOR shall promptly refund the disallowed amount to COUNTY, or, at its option, COUNTY may offset the amount disallowed from any payment due to CONTRACTOR.

B.1 OBJECTIVE: JUMP Technology Services, to provide a Software-as-a-Service (SaaS) solution including all maintenance and support, to enhance ASD's ability to receive, respond to, and document reports of dependent and elder adult abuse. The system will integrate with County systems and serve as a comprehensive information-management platform. Support and maintenance requirements are detailed in V, JUMP's Enterprise Subscription Agreement.

B.2 COUNTY RESPONSIBILITIES

County shall:

A. Request technical support and Help Desk Tickets (HDT) as outlined in JUMP's Enterprise Subscription Agreement attached hereto as V.

B. Monitor the performance of the CONTRACTOR in meeting the terms, conditions and services in this Agreement. COUNTY, at its sole discretion, may monitor the performance of the CONTRACTOR through any combination of the following methods: periodic on-site visits, annual inspections, evaluations and CONTRACTOR self-monitoring.

B.3 CONTRACTOR RESPONSIBILITIES

Contractor shall provide services as set forth below:

A. Provide a Software-as-a-Service (SaaS) solution platform that delivers system maintenance, technical consulting, troubleshooting and system enhancements to enhance ASD's ability to receive, respond to, and document reports of dependent and elder adult abuse as outlined in JUMP's Enterprise Subscription Agreement, attached hereto as V, JUMP's Enterprise Subscription Agreement.

B. Service Credits:

1. The CONTRACTOR shall provide 60 service credits annually, which may be used toward additional services, such as custom query writing, custom reporting, and system modifications/enhancements. These credits are valid for one year and do not carry over to subsequent years.

2. A discretionary fund in the amount of $17,500 has been allocated for the full term of the agreement to cover costs that exceed the 60 service credits. The Enhancement budget can also be used to cover insufficient credits.

3. Use of discretionary funds must be approved by DPSS ASD prior to expenditure.

4. No work shall be completed for hourly services that are not in the contract, unless through a formally approved and executed amendment by both parties.

C. Home Safe Support

CONTRACTOR shall set up the following Home Safe data elements:

1. Track and identify Home Safe clients.

2. Provide mapped data elements from Home Safe Assessments to populate the HSAPS19.
3. Maintain an intervention-tracking table to ensure aggregate data is accurately captured and reported.
4. Track reports to help programs identify 6- and 12-month follow-ups.
5. Update reporting tables in real time.
6. Provide a shared portal for community partners and supporting data administrators.
7. Provide HSAPS19 and HMIS export.

B.4 REPORTING

A. On a weekly basis and/or as requested, CONTRACTOR shall make available to the COUNTY a complete and secure (i.e. encrypted and appropriated authenticated) download file of COUNTY Data in XML format including all schema and transformation definitions and/or delimited text files with documented, detailed schema definitions along with attachments in their native format.

B. CONTRACTOR shall provide the COUNTY with reports documenting Uptime and Downtime, as requested.

C. CONTRACTOR shall provide ongoing Home Safe data and reporting support for LEAPS.

D. CONTRACTOR shall provide the COUNTY with access to license limit reports each month to assist in monitoring the license level. This report shall be available by the 15th day of each month.

E. CONTRACTOR shall provide a monthly report of the service credits that summarizes the following:

1. Credits used during the month
2. Credits currently in progress which includes the purpose and anticipated completion date
3. Remaining credit balance for the fiscal year

B.5 JOINT OPERATION MEETINGS (JOMS)

Participate in Joint Operation Meetings (JOMS) and/or other meetings intended to evaluate program implementation and identify needed modifications where appropriate.

HIPAA Business Associate Agreement
Addendum to Contract
Between the County of Riverside and JUMP Technology Services, L.L.C.

This HIPAA Business Associate Agreement (the "Addendum") supplements and is made part of (the DPSS-0005468 "Underlying Agreement") between the County of Riverside ("County") and JUMP Technology Services, L.L.C. ("Contractor") and shall be effective as of the date the Underlying Agreement is approved by both Parties (the "Effective Date").

RECITALS

WHEREAS, County and Contractor entered into the Underlying Agreement pursuant to which the Contractor provides services to County, and in conjunction with the provision of such services certain protected health information ("PHI") and/or certain electronic protected health information ("ePHI") may be created by or made available to Contractor for the purposes of carrying out its obligations under the Underlying Agreement; and,

WHEREAS, the provisions of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), Public Law 104-191 enacted August 21, 1996, and the Health Information Technology for Economic and Clinical Health Act ("HITECH") of the American Recovery and Reinvestment Act of 2009, Public Law 111-5 enacted February 17, 2009, and the laws and regulations promulgated subsequent thereto, as may be amended from time to time, are applicable to the protection of any use or disclosure of PHI and/or ePHI pursuant to the Underlying Agreement; and,

WHEREAS, County is a covered entity, as defined in the Privacy Rule; and,

WHEREAS, to the extent County discloses PHI and/or ePHI to Contractor or Contractor creates, receives, maintains, transmits, or has access to PHI and/or ePHI of County, Contractor is a business associate, as defined in the Privacy Rule; and,

WHEREAS, pursuant to 42 USC §17931 and §17934, certain provisions of the Security Rule and Privacy Rule apply to a business associate of a covered entity in the same manner that they apply to the covered entity, the additional security and privacy requirements of HITECH are applicable to business associates and must be incorporated into the business associate agreement, and a business associate is liable for civil and criminal penalties for failure to comply with these security and/or privacy provisions; and,

WHEREAS, the parties mutually agree that any use or disclosure of PHI and/or ePHI must be in compliance with the Privacy Rule, Security Rule, HIPAA, HITECH and any other applicable law; and,

WHEREAS, the parties intend to enter into this Addendum to address the requirements and obligations set forth in the Privacy Rule, Security Rule, HITECH and HIPAA as they apply to Contractor as a business associate of County, including the establishment of permitted and required uses and disclosures of PHI and/or ePHI created or received by Contractor during the course of performing functions, services and activities on behalf of County, and appropriate limitations and conditions on such uses and disclosures;

NOW, THEREFORE, in consideration of the mutual promises and covenants contained herein, the parties agree as follows:

1. Definitions. Terms used, but not otherwise defined, in this Addendum shall have the same meaning as those terms in HITECH, HIPAA, Security Rule and/or Privacy Rule, as may be amended from time to time.

A. "Breach" when used in connection with PHI means the acquisition, access, use or disclosure of PHI in a manner not permitted under subpart E of the Privacy Rule which compromises the security or privacy of the PHI, and shall have the meaning given such term in 45 CFR §164.402.

(1) Except as provided below in Paragraph (2) of this definition, acquisition, access, use, or disclosure of PHI in a manner not permitted by subpart E of the Privacy Rule is presumed to be a breach unless Contractor demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment of at least the following four factors:

(a) The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;

(b) The unauthorized person who used the PHI or to whom the disclosure was made;

(c) Whether the PHI was actually acquired or viewed; and

(d) The extent to which the risk to the PHI has been mitigated.

(2) Breach excludes:

(a) Any unintentional acquisition, access or use of PHI by a workforce member or person acting under the authority of a covered entity or business associate, if such acquisition, access or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under subpart E of the Privacy Rule.

(b) Any inadvertent disclosure by a person who is authorized to access PHI at a covered entity or business associate to another person authorized to access PHI at the same covered entity, business associate, or organized health care arrangement in which County participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted by subpart E of the Privacy Rule.

(c) A disclosure of PHI where a covered entity or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

B. "Business associate" has the meaning given such term in 45 CFR §164.501, including but not limited to a subcontractor that creates, receives, maintains, transmits or accesses PHI on behalf of the business associate.

C. "Data aggregation" has the meaning given such term in 45 CFR §164.501.

D. "Designated record set" as defined in 45 CFR §164.501 means a group of records maintained by or for a covered entity that may include: the medical records and billing records about individuals maintained by or for a covered health care provider; the enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or, used, in whole or in part, by or for the covered entity to make decisions about individuals.

E. "Electronic protected health information" ("ePHI") as defined in 45 CFR §160.103 means protected health information transmitted by or maintained in electronic media.

F. "Electronic health record" means an electronic record of health-related information on an individual that is created, gathered, managed, and consulted by authorized health care clinicians and staff, and shall have the meaning given such term in 42 USC §17921(5).

G. "Health care operations" has the meaning given such term in 45 CFR §164.501.

H. "Individual" as defined in 45 CFR §160.103 means the person who is the subject of protected health information.

I. "Person" as defined in 45 CFR §160.103 means a natural person, trust or estate, partnership, corporation, professional association or corporation, or other entity, public or private.

J. "Privacy Rule" means the HIPAA regulations codified at 45 CFR Parts 160 and 164, Subparts A 17 and E.

K. "Protected health information" ("PHI") has the meaning given such term in 45 CFR §160.103, which includes ePHI.

L. "Required by law" has the meaning given such term in 45 CFR §164.103.

M. "Secretary" means the Secretary of the U.S. Department of Health and Human Services 22 ("HHS").

N. "Security incident" as defined in 45 CFR §164.304 means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

O. "Security Rule" means the HIPAA Regulations codified at 45 CFR Parts 160 and 164, Subparts 27 A and C.

P. "Subcontractor" as defined in 45 CFR §160.103 means a person to whom a business associate delegates a function, activity, or service, other than in the capacity of a member of the workforce of such business associate.

Q. "Unsecured protected health information" and "unsecured PHI" as defined in 45 CFR §164.402 means PHI not rendered unusable, unreadable, or indecipherable to unauthorized persons through use of a technology or methodology specified by the Secretary in the guidance issued 34 under 42 USC §17932(h)(2).

2. Scope of Use and Disclosure by Contractor of County's PHI and/or ePHI.

A. Except as otherwise provided in this Addendum, Contractor may use, disclose, or access PHI and/or ePHI as necessary to perform any and all obligations of Contractor under the Underlying Agreement or to perform functions, activities or services for, or on behalf of, County as specified in this Addendum, if such use or disclosure does not violate HIPAA, HITECH, the Privacy Rule and/or Security Rule.

B. Unless otherwise limited herein, in addition to any other uses and/or disclosures permitted or authorized by this Addendum or required by law, in accordance with 45 CFR §164.504(e)(2), Contractor may:

(1) Use PHI and/or ePHI if necessary for Contractor's proper management and administration and to carry out its legal responsibilities; and,

(2) Disclose PHI and/or ePHI for the purpose of Contractor's proper management and administration or to carry out its legal responsibilities, only if:

(a) The disclosure is required by law; or,

(b) Contractor obtains reasonable assurances, in writing, from the person to whom Contractor will Hold such PHI disclose such PHI and/or ePHI that the person will:

(i) and/or ePHI in confidence and use or further disclose it only for the purpose for which Contractor disclosed it to the person, or as required by law; and,

(ii) Notify Contractor of any instances of which it becomes aware in which the confidentiality of the information has been breached; and,

(3) Use PHI to provide data aggregation services relating to the health care operations of County pursuant to the Underlying Agreement or as requested by County; and,

(4) De-identify all PHI and/or ePHI of County received by Contractor under this Addendum provided that the de-identification conforms to the requirements of the Privacy Rule and/or 24 Security Rule and does not preclude timely payment and/or claims processing and receipt.

C. Notwithstanding the foregoing, in any instance where applicable state and/or federal laws and/or regulations are more stringent in their requirements than the provisions of HIPAA, including, but not limited to, prohibiting disclosure of mental health and/or substance abuse records, the applicable state and/or federal laws and/or regulations shall control the disclosure of records.

3. Prohibited Uses and Disclosures.

A. Contractor may neither use, disclose, nor access PHI and/or ePHI in a manner not authorized by the Underlying Agreement or this Addendum without patient authorization or de-identification of the PHI and/or ePHI and as authorized in writing from County.

B. Contractor may neither use, disclose, nor access PHI and/or ePHI it receives from County or from another business associate of County, except as permitted or required by this Addendum, or as required by law.

C. Contractor agrees not to make any disclosure of PHI and/or ePHI that County would be prohibited from making.

D. Contractor shall not use or disclose PHI for any purpose prohibited by the Privacy Rule, Security Rule, HIPAA and/or HITECH, including, but not limited to 42 USC §17935 and §17936. Contractor agrees:

(1) Not to use or disclose PHI for fundraising, unless pursuant to the Underlying Agreement and only if permitted by and in compliance with the requirements of 45 CFR §164.514(f) or 45 CFR §164.508;

(2) Not to use or disclose PHI for marketing, as defined in 45 CFR §164.501, unless pursuant tothe Underlying Agreement and only if permitted by and in compliance with the requirements of 45 CFR §164.508(a)(3);

(3) Not to disclose PHI, except as otherwise required by law, to a health plan for purposes of carrying out payment or health care operations, if the individual has requested this restriction pursuant to 42 USC §17935(a) and 45 CFR §164.522, and has paid out of pocket in full for the health care item or service to which the PHI solely relates; and,

(4) Not to receive, directly or indirectly, remuneration in exchange for PHI, or engage in any act that would constitute a sale of PHI, as defined in 45 CFR §164.502(a)(5)(ii), unless permitted by the Underlying Agreement and in compliance with the requirements of a valid authorization under 45 CFR §164.508(a)(4). This prohibition shall not apply to payment by County to Contractor for services provided pursuant to the Underlying Agreement.

4. Obligations of County.

A. County agrees to make its best efforts to notify Contractor promptly in writing of any restrictions on the use or disclosure of PHI and/or ePHI agreed to by County that may affect Contractor's ability to perform its obligations under the Underlying Agreement, or this Addendum.

B. County agrees to make its best efforts to promptly notify Contractor in writing of any changes in, or revocation of, permission by any individual to use or disclose PHI and/or ePHI, if such changes or revocation may affect Contractor's ability to perform its obligations under the Underlying Agreement, or this Addendum.

C. County agrees to make its best efforts to promptly notify Contractor in writing of any known limitation(s) in its notice of privacy practices to the extent that such limitation may affect Contractor's use or disclosure of PHI and/or ePHI.

D. County agrees not to request Contractor to use or disclose PHI and/or ePHI in any manner that would not be permissible under HITECH, HIPAA, the Privacy Rule, and/or Security Rule.

E. County agrees to obtain any authorizations necessary for the use or disclosure of PHI and/or ePHI, so that Contractor can perform its obligations under this Addendum and/or Underlying Agreement.

5. **Obligations of Contractor.** In connection with the use or disclosure of PHI and/or ePHI, Contractor agrees to:

   A. Use or disclose PHI only if such use or disclosure complies with each applicable requirement of45 CFR §164.504(e). Contractor shall also comply with the additional privacy requirements that are applicable to covered entities in HITECH, as may be amended from time to time.

   B. Not use or further disclose PHI and/or ePHI other than as permitted or required by this Addendum or as required by law. Contractor shall promptly notify County if Contractor is required by law to disclose PHI and/or ePHI.

   C. Use appropriate safeguards and comply, where applicable, with the Security Rule with respect to ePHI, to prevent use or disclosure of PHI and/or ePHI other than as provided for by this Addendum.

   D. Mitigate, to the extent practicable, any harmful effect that is known to Contractor of a use or disclosure of PHI and/or ePHI by Contractor in violation of this Addendum.

   E. Report to County any use or disclosure of PHI and/or ePHI not provided for by this Addendum or otherwise in violation of HITECH, HIPAA, the Privacy Rule, and/or Security Rule of which Contractor becomes aware, including breaches of unsecured PHI as required by 45 CFR §164.410.

   F. In accordance with 45 CFR §164.502(e)(1)(ii), require that any subcontractors that create, receive, maintain, transmit or access PHI on behalf of the Contractor agree through contract to the same restrictions and conditions that apply to Contractor with respect to such PHI and/or ePHI, including the restrictions and conditions pursuant to this Addendum.

   G. Make available to County or the Secretary, in the time and manner designated by County or Secretary, Contractor's internal practices, books and records relating to the use, disclosure and privacy protection of PHI received from County, or created or received by Contractor on behalf of County, for purposes of determining, investigating or auditing Contractor's and/or County's compliance with the Privacy Rule.

   H. Request, use or disclose only the minimum amount of PHI necessary to accomplish the intended purpose of the request, use or disclosure in accordance with 42 USC §17935(b) and 45 CFR §164.502(b)(1).

   I. Comply with requirements of satisfactory assurances under 45 CFR §164.512 relating to notice or qualified protective order in response to a third party's subpoena, discovery request, or other lawful process for the disclosure of PHI, which Contractor shall promptly notify County upon Contractor's receipt of such request from a third party.

   J. Not require an individual to provide patient authorization for use or disclosure of PHI as a condition for treatment, payment, enrollment in any health plan (including the health plan administered by County), or eligibility of benefits, unless otherwise excepted under 45 CFR §164.508(b)(4) and authorized in writing by County.

   K. Use appropriate administrative, technical and physical safeguards to prevent inappropriate use, disclosure, or access of PHI and/or ePHI.

L. Obtain and maintain knowledge of applicable laws and regulations related to HIPAA and HITECH, as may be amended from time to time.

M. Comply with the requirements of the Privacy Rule that apply to the County to the extent Contractor is to carry out County's obligations under the Privacy Rule.

N. Take reasonable steps to cure or end any pattern of activity or practice of its subcontractor of which Contractor becomes aware that constitute a material breach or violation of the subcontractor's obligations under the business associate contract with Contractor, and if such steps are unsuccessful, Contractor agrees to terminate its contract with the subcontractor if feasible.

6. Access to PHI, Amendment and Disclosure Accounting. Contractor agrees to:

A. **Access to PHI, including ePHI.** Provide access to PHI, including ePHI if maintained electronically, in a designated record set to County or an individual as directed by County, within five (5) days of request from County, to satisfy the requirements of 45 CFR §164.524.

B. **Amendment of PHI.** Make PHI available for amendment and incorporate amendments to PHI in a designated record set County directs or agrees to at the request of an individual, within fifteen (15) days of receiving a written request from County, in accordance with 45 CFR §164.526.

C. **Accounting of disclosures of PHI and electronic health record.** Assist County to fulfill its obligations to provide accounting of disclosures of PHI under 45 CFR §164.528 and, where applicable, electronic health records under 42 USC §17935(c) if Contractor uses or maintains electronic health records. Contractor shall:

(1) Document such disclosures of PHI and/or electronic health records, and information related to such disclosures, as would be required for County to respond to a request by an individual for an accounting of disclosures of PHI and/or electronic health record in accordance with 45 CFR §164.528.

(2) Within fifteen (15) days of receiving a written request from County, provide to County or any individual as directed by County information collected in accordance with this section to permit County to respond to a request by an individual for an accounting of disclosures of PHI and/or electronic health record.

(3) Make available for County information required by this Section 6.C for six (6) years preceding the individual's request for accounting of disclosures of PHI, and for three (3) years preceding the individual's request for accounting of disclosures of electronic health record.

7. Security of ePHI. In the event County discloses ePHI to Contractor or Contractor needs to create, receive, maintain, transmit or have access to County ePHI, in accordance with 42 USC §17931 and 45 CFR §164.314(a)(2)(i), and §164.306, Contractor shall:

A. Comply with the applicable requirements of the Security Rule, and implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of ePHI that Contractor creates, receives, maintains, or transmits on behalf of County in accordance with 45 CFR §164.308, §164.310, and §164.312;

B. Comply with each of the requirements of 45 CFR §164.316 relating to the implementation of policies, procedures and documentation requirements with respect to ePHI;

C. Protect against any reasonably anticipated threats or hazards to the security or integrity of ePHI;

D. Protect against any reasonably anticipated uses or disclosures of ePHI that are not permitted or required under the Privacy Rule;

E. Ensure compliance with the Security Rule by Contractor's workforce;

F. In accordance with 45 CFR §164.308(b)(2), require that any subcontractors that create, receive, maintain, transmit, or access ePHI on behalf of Contractor agree through contract to the same restrictions and requirements contained in this Addendum and comply with the applicable requirements of the Security Rule;

G. Report to County any security incident of which Contractor becomes aware, including breaches of unsecured PHI as required by 45 CFR §164.410; and,

H. Comply with any additional security requirements that are applicable to covered entities in Title 42 (Public Health and Welfare) of the United States Code, as may be amended from time to time, including but not limited to HITECH.

8. **Breach of Unsecured PHI.** In the case of breach of unsecured PHI, Contractor shall comply with the applicable provisions of 42 USC §17932 and 45 CFR Part 164, Subpart D, including but not limited to 45 CFR §164.410.

A. **Discovery and notification.** Following the discovery of a breach of unsecured PHI, Contractor shall notify County in writing of such breach without unreasonable delay and in no case later than 60 calendar days after discovery of a breach, except as provided in 45 CFR §164.412.

(1) **Breaches treated as discovered.** A breach is treated as discovered by Contractor as of the first day on which such breach is known to Contractor or, by exercising reasonable diligence, would have been known to Contractor, which includes any person, other than the person committing the breach, who is an employee, officer, or other agent of Contractor (determined in accordance with the federal common law of agency).

(2) **Content of notification.** The written notification to County relating to breach of unsecured PHI shall include, to the extent possible, the following information if known (or can be reasonably obtained) by Contractor:

(a) The identification of each individual whose unsecured PHI has been, or is reasonably believed by Contractor to have been accessed, acquired, used or disclosed during the breach;

(b) A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;

(c) A description of the types of unsecured PHI involved in the breach, such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved;

(d) Any steps individuals should take to protect themselves from potential harm resulting from the breach;

(e) A brief description of what Contractor is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches; and,

(f) Contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, web site, or postal address.

B. **Cooperation.** With respect to any breach of unsecured PHI reported by Contractor, Contractor shall cooperate with County and shall provide County with any information requested by County to enable County to fulfill in a timely manner its own reporting and notification obligations, including but not limited to providing notice to individuals, prominent media outlets and the Secretary in accordance with 42 USC §17932 and 45 CFR §164.404, §164.406 and §164.408.

C. **Breach log.** To the extent breach of unsecured PHI involves less than 500 individuals, Contractor shall maintain a log or other documentation of such breaches and provide such log or other documentation on an annual basis to County not later than fifteen (15) days after the end of each calendar year for submission to the Secretary.

D. **Delay of notification authorized by law enforcement.** If Contractor delays notification of breach of unsecured PHI pursuant to a law enforcement official's statement that required notification, notice or posting would impede a criminal investigation or cause damage to national security, Contractor shall maintain documentation sufficient to demonstrate its compliance with the requirements of 45 CFR §164.412.

E. **Payment of costs.** With respect to any breach of unsecured PHI caused solely by the Contractor's failure to comply with one or more of its obligations under this Addendum and/or the provisions of HITECH, HIPAA, the Privacy Rule or the Security Rule, Contractor agrees to pay any and all costs associated with providing all legally required notifications to individuals, media outlets, and the Secretary. This provision shall not be construed to limit or diminish Contractor's obligations to indemnify, defend and hold harmless County under Section 9 of this Addendum.

F. **Documentation.** Pursuant to 45 CFR §164.414(b), in the event Contractor's use or disclosure of PHI and/or ePHI violates the Privacy Rule, Contractor shall maintain documentation sufficient to demonstrate that all notifications were made by Contractor as required by 45 CFR Part 164, Subpart D, or that such use or disclosure did not constitute a breach, including Contractor's completed risk assessment and investigation documentation.

G. **Additional State Reporting Requirements.** The parties agree that this Section 8.G applies only if and/or when County, in its capacity as a licensed clinic, health facility, home health agency, or hospice, is required to report unlawful or unauthorized access, use, or disclosure of medical information under the more stringent requirements of California Health & Safety Code §1280.15. For purposes of this Section 8.G, "unauthorized" has the meaning given such term in California Health & Safety Code §1280.15(j)(2).

(1) Contractor agrees to assist County to fulfill its reporting obligations to affected patients and to the California Department of Public Health ("CDPH") in a timely manner under the California Health & Safety Code §1280.15.

(2) Contractor agrees to report to County any unlawful or unauthorized access, use, or disclosure of patient's medical information without unreasonable delay and no later than two (2) business days after Contractor detects such incident. Contractor further agrees such report shall be made in writing and shall include substantially the same types of information listed above in Section 8.A.2 (Content of Notification) as applicable to the unlawful or unauthorized access, use, or disclosure as defined above in this section, understanding and acknowledging that the term "breach" as used in Section 8.A.2 does not apply to California Health & Safety Code §1280.15.

9. Hold Harmless/Indemnification.

A. Contractor agrees to indemnify and hold harmless County, all Agencies, Districts, Special Districts and Departments of County, their respective directors, officers, Board of Supervisors, elected and appointed officials, employees, agents and representatives from any liability whatsoever, based or asserted upon any services of Contractor, its officers, employees, subcontractors, agents or representatives arising out of or in any way relating to this Addendum, including but not limited to property damage, bodily injury, death, or any other element of any kind or nature whatsoever arising from the performance of Contractor, its officers, agents, employees, subcontractors, agents or representatives from this Addendum. Contractor shall defend, at its sole expense, all costs and fees, including but not limited to attorney fees, cost of investigation, defense and settlements or awards, of County, all Agencies, Districts, Special Districts and Departments of County, their respective directors, officers, Board of Supervisors, elected and appointed officials, employees, agents or representatives in any claim or action based upon such alleged acts or omissions.

B. With respect to any action or claim subject to indemnification herein by Contractor, Contractor shall, at their sole cost, have the right to use counsel of their choice, subject to the approval of County, which shall not be unreasonably withheld, and shall have the right to adjust, settle, or compromise any such action or claim without the prior consent of County; provided, however, that any such adjustment, settlement or compromise in no manner whatsoever limits or circumscribes Contractor's indemnification to County as set forth herein. Contractor's obligation to defend, indemnify and hold harmless County shall be subject to County having given Contractor written notice within a reasonable period of time of the claim or of the commencement of the related action, as the case may be, and information and reasonable assistance, at Contractor's expense, for the defense or settlement thereof. Contractor's obligation hereunder shall be satisfied when Contractor has provided to County the appropriate form of dismissal relieving County from any liability for the action or claim involved.

C. The specified insurance limits required in the Underlying Agreement of this Addendum shall in no way limit or circumscribe Contractor's obligations to indemnify and hold harmless County herein from third party claims arising from issues of this Addendum.

D. In the event there is conflict between this clause and California Civil Code §2782, this clause shall be interpreted to comply with Civil Code §2782. Such interpretation shall not relieve the Contractor from indemnifying County to the fullest extent allowed by law.

E. In the event there is a conflict between this indemnification clause and an indemnification clause contained in the Underlying Agreement of this Addendum, this indemnification shall only apply to the subject issues included within this Addendum.

10. Term. This Addendum shall commence upon the Effective Date and shall terminate when all PHI and/or ePHI provided by County to Contractor or created or received by Contractor on behalf of County, is destroyed or returned to County, or, if it is infeasible to return or destroy PHI and/ePHI, protections are extended to such information, in accordance with section 11.B of this Addendum.

11. Termination.

A. **Termination for Breach of Contract.** A breach of any provision of this Addendum by either party shall constitute a material breach of the Underlying Agreement and will provide grounds for terminating this Addendum and the Underlying Agreement with or without an opportunity to cure the breach, notwithstanding any provision in the Underlying Agreement to the contrary. Either party, upon written notice to the other party describing the breach, may take any of the following actions:

(1) Terminate the Underlying Agreement and this Addendum, effective immediately, if the other party breaches a material provision of this Addendum.

(2) Provide the other party with an opportunity to cure the alleged material breach and in the event the other party fails to cure the breach to the satisfaction of the non-breaching party in a timely manner, the non-breaching party has the right to immediately terminate the Underlying Agreement and this Addendum.

(3) If termination of the Underlying Agreement is not feasible, the breaching party, upon the request of the non-breaching party, shall implement, at its own expense, a plan to cure the breach and report regularly on its compliance with such plan to the non-breaching party.

B. **Effect of Termination.**

(1) Upon termination of this Addendum, for any reason, Contractor shall return or, if agreed to in writing by County, destroy all PHI and/or ePHI received from County, or created or received by the Contractor on behalf of County, and, in the event of destruction, Contractor shall certify such destruction, in writing, to County. This provision shall apply to all PHI and/or ePHI which are in the possession of subcontractors or agents of Contractor. Contractor shall retain no copies of PHI and/or ePHI, except as provided below in paragraph (2) of this section.

(2) In the event that Contractor determines that returning or destroying the PHI and/or ePHI is not feasible, Contractor shall provide written notification to County of the conditions that make such return or destruction not feasible. Upon determination by Contractor that return or destruction of PHI and/or ePHI is not feasible, Contractor shall extend the protections of this Addendum to such PHI and/or ePHI and limit further uses and disclosures of such PHI and/or ePHI to those purposes which make the return or destruction not feasible, for so long as Contractor maintains such PHI and/or ePHI.

12. General Provisions.

A. **Retention Period.** Whenever Contractor is required to document or maintain documentation pursuant to the terms of this Addendum, Contractor shall retain such documentation for 6 years from the date of its creation or as otherwise prescribed by law, whichever is later.

B. **Amendment.** The parties agree to take such action as is necessary to amend this Addendum from time to time as is necessary for County to comply with HITECH, the Privacy Rule, Security Rule, and HIPAA generally.

C. **Survival.** The obligations of Contractor under Sections 3, 5, 6, 7, 8, 9, 11.B and 12.A of this Addendum shall survive the termination or expiration of this Addendum.

D. **Regulatory and Statutory References.** A reference in this Addendum to a section in HITECH, HIPAA, the Privacy Rule and/or Security Rule means the section(s) as in effect or as amended.

E. **Conflicts.** The provisions of this Addendum shall prevail over any provisions in the Underlying Agreement that conflict or appear inconsistent with any provision in this Addendum.

F. **Interpretation of Addendum.**

(1) This Addendum shall be construed to be part of the Underlying Agreement as one document. The purpose is to supplement the Underlying Agreement to include the requirements of the Privacy Rule, Security Rule, HIPAA and HITECH.

(2) Any ambiguity between this Addendum and the Underlying Agreement shall be resolved to permit County to comply with the Privacy Rule, Security Rule, HIPAA and HITECH generally.

G. **Notices to County.** All notifications required to be given by Contractor to County pursuant to the terms of this Addendum shall be made in writing and delivered to the County both by fax and to both of the addresses listed below by either registered or certified mail return receipt requested or guaranteed overnight mail with tracing capability, or at such other address as County may hereafter designate. All notices to County provided by Contractor pursuant to this Section shall be deemed given or made when received by County.

County HIPAA Privacy Officer: HIPAA Privacy Manager

County HIPAA Privacy Officer Address: P.O. Box 1569
Riverside, CA 92502

County HIPAA Privacy Officer Fax Number: (951) 955-HIPAA or (951) 955-4472

— — ——— — ——— — TO BE COMPLETED BY COUNTY PERSONNEL ONLY— — ——— ——— —

County Departmental Officer: _____

County Departmental Officer Title: _____

County Department Address: _____

County Department Fax Number: _____

I. PHYSICAL SECURITY

The Contractor shall ensure PII is used and stored in an area that is physically safe from access by unauthorized persons at all times. The Contractor agrees to safeguard PII from loss, theft, or inadvertent disclosure and, therefore, agrees to:

A. Secure all areas of the Contractor facilities where staff assist in the administration of their program and use, disclose, or store PII.

B. These areas shall be restricted to only allow access to authorized individuals by using one or more of the following:
   1. Properly coded key cards
   2. Authorized door keys
   3. Official identification

C. Issue identification badges to Contractor staff.

D. Require Contractor staff to wear these badges where PII is used, disclosed, or stored.

E. Ensure each physical location, where PII is used, disclosed, or stored, has procedures and controls that ensure an individual who is terminated from access to the facility is promptly escorted from the facility by an authorized employee and access is revoked.

F. Ensure there are security guards or a monitored alarm system at all times at the Contractor facilities and leased facilities where five hundred (500) or more individually identifiable records of PII is used, disclosed, or stored. Video surveillance systems are recommended.

G. Ensure data centers with servers, data storage devices, and/or critical network infrastructure involved in the use, storage, and/or processing of PII have perimeter security and physical access controls that limit access to only authorized staff. Visitors to the data center area must be escorted at all times by authorized staff.

H. Store paper records with PII in locked spaces, such as locked file cabinets, locked file rooms, locked desks, or locked offices in facilities which are multi-use meaning that there are County and non-County functions in one building in work areas that are not securely segregated from each other. It is recommended that all PII be locked up when unattended at any time, not just within multi-use facilities.

I. Use all reasonable measures to prevent non-authorized personnel and visitors from having access to, control of, or viewing PII.

II. TECHNICAL SECURITY CONTROLS

A. Workstation/Laptop Encryption. All workstations and laptops, which use, store and/or process PII, must be encrypted using a FIPS 140-2 certified algorithm 128 bit or higher, such as Advanced Encryption Standard (AES). The encryption solution must be full disk. It is encouraged, when available and when feasible, that the encryption be 256 bit.

B. Server Security. Servers containing unencrypted PII must have sufficient administrative, physical, and technical controls in place to protect that data, based upon a risk assessment/system security review. It is recommended to follow the guidelines documented in the latest revision of the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Security and Privacy Controls for Federal Information Systems and Organizations.

C. Minimum Necessary. Only the minimum necessary amount of PII required to perform required business functions may be accessed, copied, downloaded, or exported.

D. Mobile Device and Removable Media. All electronic files, which contain PII data, must be encrypted when stored on any mobile device or removable media (i.e. USB drives, CD/DVD, smartphones, tablets, backup tapes etc.). Encryption must be a FIPS 140-2 certified algorithm 128 bit or higher, such as AES. It is encouraged, when available and when feasible, that the encryption be 256 bit.

E. Antivirus Software. All workstations, laptops and other systems, which process and/or store PII, must install and actively use an antivirus software solution. Antivirus software should have automatic updates for definitions scheduled at least daily.

F. Patch Management.
   1. All workstations, laptops and other systems, which process and/or store PII, must have critical security patches applied, with system reboot if necessary.
   2. There must be a documented patch management process that determines installation timeframe based on risk assessment and vendor recommendations.
   3. At a maximum, all applicable patches deemed as critical must be installed within thirty (30) days of vendor release. It is recommended that critical patches which are high risk be installed within seven (7) days.
   4. Applications and systems that cannot be patched within this time frame, due to significant operational reasons, must have compensatory controls implemented to minimize risk.

G. User IDs and Password Controls.
   1. All users must be issued a unique username for accessing PII.
   2. Username must be promptly disabled, deleted, or the password changed upon the transfer or termination of an employee within twenty- four (24) hours. Note: Twenty-four (24) hours is defined as one (1) working day.
   3. Passwords are not to be shared.
   4. Passwords must be at least eight (8) characters.
   5. Passwords must be a non-dictionary word.
   6. Passwords must not be stored in readable format on the computer or server.
   7. Passwords must be changed every ninety (90) days or less. It is recommended that passwords be required to be changed every sixty (60) days or less.
   8. Passwords must be changed if revealed or compromised.
   9. Passwords must be composed of characters from at least three (3) of the following four (4) groups from the standard keyboard:
      a. Upper case letters (A-Z)
      b. Lower case letters (a-z)
      c. Arabic numerals (0-9)
      d. Special characters (!@,#, etc.)

H. Data Destruction. When no longer needed, all PII must be cleared, purged, or destroyed consistent with NIST SP 800-88, Guidelines for Media Sanitization, such that the PII cannot be retrieved.

I. System Timeout. The systems providing access to PII must provide an automatic timeout, requiring re-authentication of the user session after no more than twenty (20) minutes of inactivity.

J. Warning Banners. The systems providing access to PII must display a warning banner stating, at a minimum:
   1. Data is confidential;
   2. Systems are logged;

3. System use is for business purposes only, by authorized users; and
4. Users shall log off the system immediately if they do not agree with these requirements.

K. System Logging.
   1. The systems which provide access to PII must maintain an automated audit trail that can identify the user or system process which initiates a request for PII, or alters PII.
   2. The audit trail shall:
      a. Be date and time stamped;
      b. Log both successful and failed accesses;
      c. Be read-access only; and
      d. Be restricted to authorized users.
      3. If PII is stored in a database, database logging functionality shall be enabled.
      4. Audit trail data shall be archived for at least three (3) years from the occurrence.

L. Access Controls. The system providing access to PII shall use role-based access controls for all user authentications, enforcing the principle of least privilege.

M. Transmission Encryption.
   1. All data transmissions of PII outside of a secure internal network must be encrypted using a Federal Information Processing Standard (FIPS) 140-2 certified algorithm that is 128 bit or higher, such as Advanced Encryption Standard (AES) or Transport Layer Security (TLS). It is encouraged, when available and when feasible, that 256 bit encryption be used.
   2. Encryption can be end to end at the network level, or the data files containing PII can be encrypted.
   3. This requirement pertains to any type of PII in motion such as website access, file transfer, and email.

N. Intrusion Prevention. All systems involved in accessing, storing, transporting, and protecting PII, which are accessible through the Internet, must be protected by an intrusion detection and prevention solution.

III. AUDIT CONTROLS

A. System Security Review.
   1. The Contractor must ensure audit control mechanisms are in place.
   2. All systems processing and/or storing PII must have at least an annual system risk assessment/security review that ensures administrative, physical, and technical controls are functioning effectively and provide an adequate level of protection.
   3. Reviews should include vulnerability scanning tools.

B. Log Reviews. All systems processing and/or storing PII must have a process or automated procedure in place to review system logs for unauthorized access.

C. Change Control. All systems processing and/or storing PII must have a documented change control process that ensures separation of duties and protects the confidentiality, integrity and availability of data.

IV. BUSINESS CONTINUITY / DISASTER RECOVERY CONTROLS

A. Emergency Mode Operation Plan. The Contractor must establish a documented plan to enable continuation of critical business processes and protection of the security of PII kept in an electronic format in the event of an emergency. Emergency means any circumstance or situation that causes normal computer operations to become unavailable for use in performing the work required under this Agreement for more than twenty-four (24) hours.

B. Data Centers. Data centers with servers, data storage devices, and critical network infrastructure involved in the use, storage and/or processing of PII, must include environmental protection such as cooling, power, and fire prevention, detection, and suppression.

C. Data Backup and Recovery Plan.
   1. The Contractor shall have established documented procedures to backup PII to maintain retrievable exact copies of PII.
   2. The documented backup procedures shall contain a schedule which includes incremental and full backups.
   3. The procedures shall include storing backups offsite.
   4. The procedures shall ensure an inventory of backup media.
   5. The Contractor shall have established documented procedures to recover PII data.
   6. The documented recovery procedures shall include an estimate of the amount of time needed to restore the PII data.

V. PAPER DOCUMENT CONTROLS

A. Supervision of Data. The PII in paper form shall not be left unattended at any time, unless it is locked in a file cabinet, file room, desk or office. Unattended means that information may be observed by an individual not authorized to access the information.

B. Data in Vehicles. The Contractor shall have policies that include, based on applicable risk factors, a description of the circumstances under which staff can transport PII, as well as the physical security requirements during transport. A Contractor that chooses to permit its staff to leave records unattended in vehicles must include provisions in its policies to ensure the PII is stored in a non-visible area such as a trunk, that the vehicle is locked, and under no circumstances permit PII be left unattended in a vehicle overnight or for other extended periods of time.

C. Public Modes of Transportation. The PII in paper form shall not be left unattended at any time in airplanes, buses, trains, etc., including baggage areas. This should be included in training due to the nature of the risk.

D. Escorting Visitors. Visitors to areas where PII is contained shall be escorted, and PII shall be kept out of sight while visitors are in the area.

E. Confidential Destruction. PII must be disposed of through confidential means, such as cross cut shredding or pulverizing.

F. Removal of Data. The PII must not be removed from the premises except for identified routine business purposes or with express written permission of the County.

G. Faxing.
   1. Faxes containing PII shall not be left unattended and fax machines shall be in secure areas.
   2. Faxes shall contain a confidentiality statement notifying persons receiving faxes in error to destroy them and notify the sender.
   3. Fax numbers shall be verified with the intended recipient before sending the fax.

H. Mailing.
   1. Mailings containing PII shall be sealed and secured from damage or inappropriate viewing of PII to the extent possible.
   2. Mailings that include five hundred (500) or more individually identifiable records containing PII in a single package shall be sent using a tracked mailing method that includes verification of delivery and receipt, unless the Contractor obtains prior written permission from the County to use another method.

VI. NOTIFICATION AND INVESTIGATION OF BREACHES AND SECURITY INCIDENTS

During the term of this Agreement, the Contractor agrees to implement reasonable systems for the discovery and prompt reporting of any Breach or Security Incident, and to take the following steps:

The Contractor shall immediately notify the County when it discovers that there may have been a breach in security which has or may have resulted in compromise to confidential data. For purposes of this section, immediately is defined as within two hours of discovery. The County contact for such notification is as follows:

Breaches should be referred to:

DPSS Privacy Officer
DESC/Employee Development Unit
Riverside County Department of Public Social Services
10281 Kidd Street
Riverside, CA 92503
Privacyincident@rivco.org

Attachment III
Medi-Cal Privacy & Security Agreement

**MEDI-CAL PRIVACY AND SECURITY AGREEMENT BETWEEN
the California Department of Health Care Services and the
County of Riverside, Department of Public Social Services**

PREAMBLE

The Department of Health Care Services (DHCS) and the Riverside County of Department of Public Social Services enter into this Medi-Cal Data Privacy and Security Agreement (Agreement) in order to ensure the privacy and security of Medi-Cal Personally Identifiable Information (PII). DHCS receives federal funding to administer California's Medicaid Program (Medi-Cal). County Department assists in the administration of Medi-Cal, in that DHCS and County Department access DHCS eligibility information for the purpose of determining eligibility for Medi-Cal. This Agreement covers the County of Riverside, Department of workers, who assist in the administration of Medi-Cal; and access, use, or disclose Medi-Cal PII.

DEFINITIONS

For the purpose of this Agreement, the following terms mean:

1. "Assist in the Administration of Medi-Cal" is performing an administrative function on behalf of Medi-Cal, and includes, but is not limited to, activities such as establishing eligibility and methods of reimbursement; determining the amount of medical assistance; providing services for recipients; conducting or assisting an investigation, prosecution, or civil or criminal proceeding related to the administration of Medi-Cal; and conducting or assisting a legislative investigation or audit related to the administration of Medi-Cal;

2. "Breach" shall have the meaning given to such term under the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 ("HIPAA") and its implementing regulations under the Information Practices Act, Civil Code section 1798.29, and under the Agreement between the Social Security Administration (SSA) and DHCS, known as the Information Exchange Agreement (IEA) (Exhibit A); this definition shall include these definitions as set out below and as my be amended in the future:

   a. "Breach" means the acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E of this part which compromises the security or privacy of the protected health information." (HIPAA Regulation 45.C.F.R. 164.402);

   b. - Breach of the security of the system' means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the agency." (Civil C. § 1798.23 (d));

   c. Breach "refers to actual loss, loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for other than authorized purposes have access have access or potential access to PII or Covered Information, whether physical, electronic, or in spoken work or recording." (IEA, Attachment 4, Electronic Information Exchange Security Requirements, Guidelines, and Procedures for Federal, State and Local Agencies Exchanging Electronic Information with the Social Security Administration, Exhibit. A).

   3. "County Worker" means those county employees, contractors, subcontractors, vendors and agents performing job functions for the County that require access to and/or use of Medi-Cal PII and that are authorized by the County to access and use Medi-Cal PII.

4. "Medi-Cal PII" is information directly obtained in the course of performing an administrative function on behalf of Medi-Cal that can be used alone, or in conjunction with any other information, to identify a specific individual. PII includes any information that can be used to search for or identify individuals, or can be used to access their files, such as name, social security number, date of birth, driver's license number or identification number. PII may be electronic or paper; and

5. "Security Incident" means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of Medi-Cal PII, or interference with system operations in an information system which processes Medi-Cal PII that is under the control of the County or County's SAWS Consortium, or a contractor, subcontractor or vendor of the County.

AGREEMENTS

NOW THEREFORE, DHCS and County Department mutually agree as follows:

I. PRIVACY AND CONFIDENTIALITY

A. County Department workers covered by this Agreement (County Workers) may use or disclose Medi-Cal PII only as permitted in this Agreement and only to assist in the administration of Medi-Cal in accordance with Welfare and Institutions Code section 14100.2 and 42 Code of Federal Regulations section 431.300 et.seq., or as required by law. Disclosures, which are required by law, such as a court order, or are made with the explicit written authorization of the Medi-Cal client, are allowable. Any other use or disclosure of Medi-Cal PII requires the express approval in writing of DHCS. No County Worker shall duplicate, disseminate or disclose Medi-Cal PII except as allowed in this Agreement.

B. Pursuant to this Agreement, County Workers may use Medi-Cal PII only to perform administrative functions related to determining eligibility for individuals applying for Medi-Cal.

C. Access to Medi-Cal PII shall be restricted to only County Workers, who need the Medi-Cal PII to perform their official duties to assist in the administration of Medi-Cal.

D. County Workers, who access, disclose or use Medi-Cal PII in a manner or for a purpose not authorized by this Agreement may be subject to civil and criminal sanctions contained in applicable federal and state statutes.

II. PERSONNEL CONTROLS

The County Department agrees to advise County Workers, who have access to Medi-Cal PII of the confidentiality of the information, the safeguards required to protect the information, and the civil and criminal sanctions for non-compliance contained in applicable federal and state laws. For that purpose, the County Department shall:

A. **Employee Training.** Train and use reasonable measures to ensure compliance with the requirements of this Agreement by County Workers, who assist in the administration of Medi-Cal and use or disclose Medi-Cal PII, including;
   1. Provide privacy and security awareness training to each new County Worker within 30 days of employment and thereafter, provide ongoing refresher training or reminders of the privacy and security safeguards in this Agreement to all County Workers, who assist in the administration of Medi-Cal and use or disclose Medi-Cal PII at least annually;
   2. Maintain records indicating each County Worker's name and the date on which the privacy and security awareness training was completed;
   3. Retain the most recent training records for a period of three years after completion of the training.

B. Employee Discipline. Apply appropriate sanctions against workforce members, who fail to comply with privacy policies and procedures or any provisions of these requirements, including termination of employment where appropriate.

C. Confidentiality Statement. Ensure that all County Workers, who assist in the administration of Medi-Cal, and use or disclose Medi-Cal PII, sign a confidentiality statement. The statement shall include at a minimum, General Use, Security and Privacy Safeguards, Unacceptable Use, and Enforcement Policies. The statement shall be signed by County Workers prior to accessing Medi-Cal PII and the most recent version shall be retained for a period of three years.

D. Background Check. Conduct a background screening of a County Worker before a County Worker may access DHCS PII. The screening should be commensurate with the risk and magnitude of harm the employee could cause, with more thorough screening being done for those employees, who are authorized to bypass significant technical and operational security controls. County Department shall retain each County Worker's most recent background check documentation for a period of three years.

III. MANAGEMENT OVERSIGHT AND MONITORING

County Department agrees to:

A. Establish and maintain ongoing management oversight and quality assurance for monitoring workforce compliance with the privacy and security safeguards in this Agreement when using or disclosing Medi-Cal PII.

B. Ensure ongoing management oversight including periodic self-assessments and random sampling of work activity by County Workers, who assist in the administration of Medi-Cal and use or disclose Medi-Cal PII. DHCS shall provide the County Department with information on the Medi-Cal Eligibility Data System (MEDS) usage anomalies for investigation and follow-up.

C. Ensure these management oversight and monitoring activities are performed by County Workers, whose job functions are separate from those, who use or disclose Medi-Cal PII as part of their routine duties.

IV. INFORMATION SECURITY AND PRIVACY STAFFING

The County agrees to:

A. Designate information security and privacy officials who are accountable for compliance with these and all other applicable requirements stated in this agreement.

B. Assign county workers to be responsible for administration and monitoring of all security related controls stated in this Agreement.

V. PHYSICAL SECURITY

County Department shall ensure Medi-Cal PII is used and stored in an area that is physically safe from access by unauthorized persons during working hours and non-working hours. County Department agrees to safeguard Medi-Cal PII from loss, theft, or inadvertent disclosure and, therefore, agrees to:

A. Secure all areas of County Department facilities where County Workers assist in the administration of Medi-Cal and use or disclose Medi-Cal PII. The County Department shall ensure these secured areas are only accessed by authorized individuals with properly coded key cards, authorized door keys or access authorization; and access to premises is by official identification.

B. Issue County Workers, who assist in the administration of Medi-Cal identification badges and require County Workers to wear these badges at County Department facilities where Medi-Cal PII is stored or used.

C. Ensure each physical location, where Medi-Cal PII is used or stored, has procedures and controls that ensure an individual, who is terminated from access to the facility is promptly escorted from the facility by an authorized employee and access is revoked.

D. Ensure there are security guards or a monitored alarm system with or without security cameras 24 hours a day, 7 days a week at County Department facilities and leased facilities where a large volume of Medi- Cal PII is stored.

E. Ensure data centers with servers, data storage devices, and critical network infrastructure involved in the use or storage of Medi-Cal PII have perimeter security and access controls that limit access to only authorized Information Technology (IT) staff. Visitors to the data center area must be escorted by authorized IT staff at all times.

F. Store paper records with Medi-Cal PII in locked spaces, such as locked file cabinets, locked file rooms, locked desks or locked offices in facilities which are multi-use, meaning that there are County Department and non-County Department functions in one building in work areas that are not securely segregated from each other. County Department shall have policies that indicate County Workers are not to leave records with Medi- Cal PII unattended at any time in vehicles or airplanes and not to check such
records in baggage on commercial airplanes.

G. Use all reasonable measures to prevent non-authorized personnel and visitors from having access to, control of, or viewing Medi-Cal PII.

VI. TECHNICAL SECURITY CONTROLS

A. Workstation/Laptop encryption. All workstations and laptops, which store Medi-Cal PII either directly or temporarily, must be encrypted using a FIPS 140-2 certified algorithm 128bit or higher, such as Advanced Encryption Standard (AES). The encryption solution must be full disk.

B. Server Security. Servers containing unencrypted Medi-Cal PII must have sufficient administrative, physical, and technical controls in place to protect that data, based upon a risk assessment/system security review.

C. Minimum Necessary. Only the minimum necessary amount of Medi-Cal PII required to perform necessary business functions may be copied, downloaded, or exported.

D. Removable media devices. All electronic files, which contain Medi-Cal PII data, must be encrypted when stored on any removable media or portable device (i.e. USB thumb drives, floppies, CD/DVD, smartphones, backup tapes etc.). Encryption must be a FIPS 140-2 certified algorithm 128bit or higher, such as AES.

E. Antivirus software. All workstations, laptops and other systems, which process and/or store Medi-Cal PII, must install and actively use comprehensive anti-virus software solution with automatic updates scheduled at least daily.

F. Patch Management. All workstations, laptops and other systems, which process and/or store Medi-Cal PII, must have critical security patches applied, with system reboot if necessary. There must be a documented patch management process that determines installation timeframe based on risk assessment and vendor recommendations. At a maximum, all applicable patches deemed as high risk must be installed within 30 days of vendor release. Applications and systems that cannot be patched within this time frame, due to significant operational reasons, must have compensatory controls implemented to minimize risk.

G. User IDs and Password Controls. All users must be issued a unique username for accessing Medi-Cal PII. Username must be promptly disabled, deleted, or the password changed upon the transfer or termination of an employee with knowledge of the password, at maximum within 24 hours. Passwords are not to be shared. Passwords must be at least eight characters and must be a non-dictionary word. Passwords must not be stored in readable format on the computer. Passwords must be changed every 90 days, preferably every 60 days. Passwords must be changed if revealed or compromised. Passwords must be composed of characters from at least three of the following four groups from the standard keyboard:

- Upper case letters (A-Z)
- Lower case letters (a-z)
- Arabic numerals (0-9)
- Non-alphanumeric characters (punctuation symbols)

H. User Access. Exercise management control and oversight, in conjunction with DHCS, of the function of authorizing individual user access to Social Security Administration (SSA) data, MEDS, and over the process of issuing and maintaining access control numbers and passwords.

I. Data Destruction. When no longer needed, all Medi-Cal PII must be wiped using the Gutmann or U.S. Department of Defense (DoD) 5220.22-M (7 Pass) standard, or by degaussing. Media may also be physically destroyed in accordance with NIST Special Publication 800-88.

J. System Timeout. The system providing access to Medi-Cal PII must provide an automatic timeout, requiring re-authentication of the user session after no more than 20 minutes of inactivity.

K. Warning Banners. All systems providing access to Medi-Cal PII must display a warning banner stating that data is confidential, systems are logged, and system use is for business purposes only by authorized users. User must be directed to log off the system if they do not agree with these requirements.

L. System Logging. The system must maintain an automated audit trail that can identify the user or system process, initiates a request for Medi-Cal PII, or alters Medi-Cal PII. The audit trail must be date and time stamped, must log both successful and failed accesses, must be read only, and must be restricted to authorized users. If Medi-Cal PII is stored in a database, database logging functionality must be enabled. Audit trail data must be archived for at least three years after occurrence.

M. Access Controls. The system providing access to Medi-Cal PII must use role based access controls for all user authentications, enforcing the principle of least privilege.

N. Transmission encryption. All data transmissions of Medi-Cal PII outside the secure internal network must be encrypted using a FIPS 140-2 certified algorithm that is 128bit or higher, such as AES. Encryption can be end to end at the network level, or the data files containing Medi-Cal PII can be encrypted. This requirement pertains to any type of Medi-Cal PII in motion such as website access, file transfer, and E-Mail.

0. Intrusion Detection. All systems involved in accessing, holding, transporting, and protecting Medi-Cal PII, which are accessible through the Internet, must be protected by a comprehensive intrusion detection and prevention solution.

VII. AUDIT CONTROLS

A. System Security Review. County Department must ensure audit control mechanisms that record and examine system activity are in place. All systems processing and/or storing Medi-Cal PII must have at least an annual system risk assessment/security review that ensures administrative, physical, and technical controls are functioning effectively and provide an adequate levels of protection. Reviews should include vulnerability scanning tools.

B. Log Reviews. All systems processing and/or storing Medi-Cal PII must have a routine procedure in place to review system logs for unauthorized access.

C. Change Control. All systems processing and/or storing Medi-Cal PII must have a documented change control procedure that ensures separation of duties and protects the confidentiality, integrity and availability of data.

D. Anomalies. Investigate anomalies in MEDS usage identified by DHCS and report conclusions of such investigations and remediation to DHCS.

VIII. BUSINESS CONTINUITY / DISASTER RECOVERY CONTROLS

A. Emergency Mode Operation Plan. County Department must establish a documented plan to enable continuation of critical business processes and protection of the security of Medi-Cal PII kept in an electronic format in the event of an emergency. Emergency means any circumstance or situation that causes normal computer operations to become unavailable for use in performing the work required under this Agreement for more than 24 hours.

B. Data Centers. Data centers with servers, data storage devices, and critical network infrastructure involved in the use or storage of Medi-Cal PII, must include sufficient environmental protection such as cooling, power, and fire prevention, detection, and suppression.

C. Data Backup Plan. County Department must have established documented procedures to backup Medi-Cal PII to maintain retrievable exact copies of Medi-Cal PII. The plan must include a regular schedule for making backups, storing backups offsite, an inventory of backup media, and an estimate of the amount of time needed to restore Medi-Cal PII should it be lost. At a minimum, the schedule must be a weekly full backup and monthly offsite storage of Medi-Cal data.

IX. PAPER DOCUMENT CONTROLS

A. Supervision of Data. Medi-Cal PII in paper form shall not be left unattended at any time, unless it is locked in a file cabinet, file room, desk or office. Unattended means that information is not being observed by an employee authorized to access the information. Medi-Cal PII in paper form shall not be left unattended at any time in vehicles or planes and shall not be checked in baggage on commercial airplanes.

B. Escorting Visitors. Visitors to areas where Medi-Cal PII is contained shall be escorted and Medi-Cal PII shall be kept out of sight while visitors are in the area.

C. Confidential Destruction. Medi-Cal PII must be disposed of through confidential means, such as cross cut shredding and pulverizing.

D. Removal of Data. Medi-Cal P11 must not be removed from the premises of County Department except for identified routine business purposes or with express written permission of DHCS.

E. Faxing. Faxes containing Medi-Cal PII shall not be left unattended and fax machines shall be in secure areas. Faxes shall contain a confidentiality statement notifying persons receiving faxes in error to destroy them. Fax numbers shall be verified with the intended recipient before sending the fax.

F. Mailing. Mailings containing Medi-Cal PII shall be sealed and secured from damage or inappropriate viewing of PII to the extent possible. Mailings that include 500 or more individually identifiable records containing Medi-Cal PII in a single package shall be sent using a tracked mailing method that includes verification of delivery and receipt, unless the prior written permission of DHCS to use another method is obtained.

X. NOTIFICATION AND INVESTIGATION OF BREACHES AND SECURITY INCIDENTS

During the term of this PSA, County Department agrees to implement reasonable systems for the discovery and prompt reporting of any Breach or Security Incident, and to take the following steps:

A. Initial Notice to DHCS. (1) To notify DHCS **immediately by telephone call plus email or fax** upon the discovery of a breach of unsecured Medi-Cal PII in electronic media or in any other media if the PII was, or is reasonably believed to have been, accessed or acquired by an unauthorized person, or upon the discovery of a suspected security incident that involves data provided to DHCS by the SSA. (2) To notify DHCS **within 24 hours by email or fax** of the discovery of any breach, security incident, intrusion, or unauthorized access, use, or disclosure of Medi-Cal PI I in violation of this Agreement and this Addendum, or potential loss of confidential data affecting this Agreement. A breach shall be treated as discovered by County Department as of the first day on which the breach is known, or by exercising reasonable diligence would have been known, to any person (other than the person committing the breach), who is an employee, officer or other agent of County Department. Notice shall be provided to the DHCS Program Contract Manager, the DHCS Privacy Officer and the DHCS Information Security Officer. If the incident occurs after business hours or on a weekend or holiday and involves electronic PII, notice shall be provided by calling the DHCS ITSD Service Desk. Notice shall be made using the "DHCS Privacy Incident Report" form, including all information known at the time. County Department shall use the most current

version of this form, which is posted on the DHCS Privacy Office website (www.dhcs.ca.pov, then select "Privacy" in the left column and then "County Use" near the middle of the page) or use this link:
http://www.dhcs.ca.gov/formsandpubs/laws/priv/Pages/CountiesOnly.aspx

Upon discovery of a breach, security incident, intrusion, or unauthorized access, use, or disclosure of Medi-Cal PI I, County Department shall take:

1. Prompt corrective action to mitigate any risks or damages involved with the breach and to protect the operating environment; and
2. Any action pertaining to such unauthorized disclosure required by applicable Federal and State laws and regulations.

B. Investigation and Investigative Report. To immediately investigate a breach, security incident, intrusion, or unauthorized access, use, or disclosure of Medi-Cal PI I, within 72 hours of the discovery, County Department shall submit an updated "DHCS Privacy Incident Report" containing the information marked with an asterisk and all other applicable information listed on the form, to the extent known at that time, to the DHCS Program Contract Manager, the DHCS Privacy Officer, and the DHCS Information Security Officer.

C. Complete Report. To provide a complete report of the investigation to the DHCS Program Contract Manager, the DHCS Privacy Officer, and the DHCS Information Security Officer within ten working days of the discovery of a breach, security incident, intrusion, or unauthorized access, use, or disclosure. The report shall be submitted on the "DHCS Privacy Incident Report" form and shall include an assessment of all known factors relevant to a determination of whether a breach occurred under applicable provisions of HIPAA, the HITECH Act, the HIPAA regulations and/or state law. The report shall also include a full, detailed corrective action plan, including information on measures that were taken to halt and/or contain the improper use or disclosure. If DHCS requests information in addition to that listed on the "DHCS Privacy Incident Report" form, County Department shall make reasonable efforts to provide DHCS with such information. If necessary, a Supplemental Report may be used to submit revised or additional information after the completed report is submitted, by submitting the revised or additional information on an updated "DHCS Privacy Incident Report" form. DHCS will review and approve the determination of whether a breach occurred, and individual notifications are required, and the corrective action plan.

D. Notification of Individuals. If the cause of a breach of Medi-Cal PII is attributable to County Department or its subcontractors, agents or vendors, County Department shall notify individuals of the breach or unauthorized use or disclosure when notification is required under state or federal law and shall pay any costs of such notifications, as well as any costs associated with the breach. The notifications shall comply with the requirements set forth in 42 U.S.C. section 17932, and its implementing regulations, including, but not limited to, the requirement that the notifications be made without unreasonable delay and in no event later than 60 calendar days. The DHCS Program Contract Manager, the DHCS Privacy Officer, and the DHCS Information Security Officer shall approve the time, manner and content of any such notifications and their review and approval must be obtained before the notifications are made.

E. Responsibility for Reporting of Breaches. If the cause of a breach of Medi-Cal PII is attributable to County Department or its agents, subcontractors or vendors, County Department is responsible for all required reporting of the breach as specified in 42 U.S.C. section 17932 and its implementing regulations, including notification to media outlets and to the Secretary, U.S. Department of Health and Human Services. If a breach of unsecured PII involves more than 500 residents of the State of California or its jurisdiction, County Department shall notify the federal Secretary, Department of Health and Human Services, of the breach immediately upon discovery of the breach. If County Department has reason to believe that duplicate reporting of the same breach or incident may occur because its subcontractors, agents or vendors may report the breach or incident to DHCS in addition to County Department, County Department shall notify DHCS, and DHCS and County Department may take appropriate action to prevent duplicate reporting.

F. DHCS Contact Information. To direct communications to the above referenced DHCS staff, the County Department shall initiate contact as indicated herein. DHCS reserves the right to make changes to the contact information below by giving written notice to the County Department. Said changes shall not require an amendment to this Addendum or the Agreement to which it is incorporated.

DHCS Program Contract Manager
DHCS Privacy Officer
DHCS Information Security Officer
Program Integrity and Security Unit Privacy Officer Information Security Officer
Policy Operations Branch do: Office of HIPAA Compliance DHCS Information Security
Medi-Cal Eligibility Division DHCS Privacy Office, MS 4722 Office, MS 6400
1501 Capitol Avenue, MS 4607 P.O. Box 997413 P.O. Box 997413
P.O. Box 997417 Sacramento, CA 95899-7413 Sacramento, CA 95899-7413
Sacramento, CA 95899-7417

Email: Email: iso@dhcs.ca.gov
Telephone: (916) 552-9200 privacyofficerdhcs.ca.cov Fax: (916) 440-5537
Telephone: (916) 445-4646 Telephone:
Fax: (916) 440-7680 ITSD Service Desk
(916) 440-7000 or (800) 579-0874

XI. COMPLIANCE WITH SSA AGREEMENT

County Department agrees to comply with substantive privacy and security requirements in the Computer Matching and Privacy Protection Act Agreement between SSA and the California Health and Human Services Agency (CHHS) and in the Agreement between SSA and DHCS, known as the Information Exchange Agreement (IEA), which are appended and hereby incorporated into this Agreement (Exhibit A). The specific sections of the IEA with substantive privacy and security requirements, which are to be complied with by County Department are in the following sections: E, Security Procedures; F. Contractor/Agent Responsibilities; G, Safeguarding and Reporting Responsibilities for PII, and in Attachment 4, Electronic Information Exchange Security Requirements, Guidelines, and Procedures for Federal, State and Local Agencies Exchanging Electronic Information with SSA. If there is any conflict between a privacy and security standard in these sections of the IEA and a standard in this Agreement, the most stringent standard shall apply. The most stringent standard means the standard which provides the greatest protection to Medi-Cal PII.

XII. COUNTY DEPARTMENT'S AGENTS AND SUBCONTRACTORS

County Department agrees to enter into written agreements with any agents, including subcontractors and vendors, to whom County Department provides Medi-Cal PII received from or created or received by County Department in performing functions or activities related to the administration of Medi-Cal that impose the same restrictions and conditions on such agents, subcontractors and vendors that apply to County Department with respect to Medi-Cal PII, including restrictions on disclosure of Medi-Cal PII and the use of appropriate administrative, physical, and technical safeguards to protect such Medi-Cal PII. County Department shall incorporate, when applicable, the relevant provisions of this PSA into each subcontract or subaward to such agents, subcontractors and vendors, including the requirement that any breach, security incident, intrusion, or unauthorized access, use, or disclosure of Medi-Cal PII be reported to County Department.

XIII. ASSESSMENTS AND REVIEWS

In order to enforce this Agreement and ensure compliance with its provisions, the County Department agrees to allow DHCS to inspect the facilities, systems, books, and records of County Department, with reasonable notice from DHCS, in order to perform assessments and reviews. Such inspections shall be scheduled at times that take into account the operational and staffing demands. County Department agrees to promptly remedy any violation of any provision of this Agreement and certify the same to the DHCS Privacy Officer and DHCS Information

Security Officer in writing, or to enter into a written corrective action plan with DHCS containing deadlines for achieving compliance with specific provisions of this Agreement.

XIV. ASSISTANCE IN LITIGATION OR ADMINISTRATIVE PROCEEDINGS

In the event of litigation or administrative proceedings involving DHCS based upon claimed violations by County Department of the privacy or security of Medi-Cal PII, or federal or state laws or agreements concerning privacy or security of Medi-Cal PII, County Department shall make all reasonable effort to make itself and County Workers assisting in the administration of Medi-Cal and using or disclosing Medi-Cal PII available to DHCS at no cost to DHCS to testify as witnesses. DHCS shall also make all reasonable efforts to make itself and any subcontractors, agents, and employees available to County Department at no cost to County Department to testify as witnesses, in the event of litigation or administrative proceedings involving County Department based upon claimed violations by DHCS of the privacy or security of Medi-Cal PII, or state or federal laws or agreements concerning privacy or security of Medi-Cal PII.

XV. AMENDMENT OF AGREEMENT

DHCS and County Department acknowledge that federal and state laws relating to data security and privacy are rapidly evolving and that amendment of this PSA may be required to provide for procedures to ensure compliance with such developments. Upon request by DHCS, County Department agrees to promptly enter into negotiations concerning an amendment to this PSA as may be needed by developments in federal and state laws and regulations. DHCS may terminate this PSA upon thirty (30) days written notice if County Department does not promptly enter into negotiations to amend this PSA when requested to do so or does not enter into an amendment that DHCS deems necessary.

XVI. TERMINATION

This PSA shall terminate three years after the date it is executed, unless the parties agree in writing to extend its term. All provisions of this PSA that provide restrictions on disclosures of Medi-Cal PII and that provide administrative, technical, and physical safeguards for the Medi-Cal PII in County Department's possession shall continue in effect beyond the termination of the PSA and shall continue until the Medi-Cal PII is destroyed or returned to DHCS.

XVII. TERMINATION FOR CAUSE

Upon DHCS' knowledge of a material breach or violation of this Agreement by User, DHCS may provide an opportunity for User to cure the breach or end the violation and may terminate this Agreement if User does not cure the breach or end the violation within the time specified by DHCS. DHCS may terminate this Agreement immediately if User has breached a material term and DHCS determines, in its sole discretion, that cure is not possible or available under the circumstances. Upon termination of this Agreement, User must destroy all PHI and PCI in accordance with Section VI.I, above. The provisions of this Agreement governing the privacy and security of the PHI and PCI shall remain in effect until all PHI and PCI is destroyed and DHCS receives a certificate of destruction.

XVIII. SIGNATORIES

The signatories below warrant and represent that they have the competent authority on behalf of their respective agencies to enter into the obligations set forth in this Agreement. The authorized officials whose signatures appear below have committed their respective agencies to the terms of this Agreement. The contract is effective on the day the final signature is obtained.

Exhibit A: Agreement between SSA and CHHS, and Agreement between SSA and DHCS with Attachment "Information System Security Guidelines for Federal, State and Local Agencies Receiving Electronic Information from the SSA." This is a sensitive document that is provided separately to the County's privacy and security office.

COUNTY OF RIVERSIDE
DEPARTMENT OF PUBLIC SOCIAL SERVICES

CONTRACTOR PAYMENT REQUEST

To: Riverside COUNTY
Department of Public Social Services
Attn: Management Reporting Unit
4060 COUNTY Circle Drive
Riverside, CA 92503

From: _____
Remit to Name

_____
Address

_____
City, State and Zip Code

_____
Contract Number

Total amount requested _____for the period of_____20 _____

Select Payment Type(s) Below:

☐ Advance Payment $_____
(if allowed by Contract/MOU)

☐ Actual Payment $ _____
(Same amount as 2076B if needed)

☐ Unit of Service Payment $_____

_____ (# of Units) x _____(Unit Price) = ($)_____

_____ (# of Units) x _____(Unit Price) = ($)_____

_____ (# of Units) x _____(Unit Price) = ($)_____

_____ (# of Units) x _____(Unit Price) = ($)_____

(# of Units) x _____(Unit Price) = ($)_____

Any questions regarding this request should be directed to and authorized by:

_____
Name Phone Number

FOR DPSS USE ONLY (DO NOT WRITE BELOW THIS LINE)

_____
MRU Authorization Date

_____
Amount Authorized

_____
Invoice Number

_____
PO Number

If amount authorized is different from the amount requested, please explain

_____

_____

_____

DEPARTMENT OF PUBLIC SOCIAL SERVICES FORMS

Mailing Instructions: When completed, these forms will summarize all of your claims for payment. Your Claims Packet will include DPSS 2076A, 2076B (if required). invoices, payroll verification, and copies of canceled checks attached, receipts, bank statements, sign-in sheets, daily logs, mileage logs, and other back-up documentation needed to comply with Contract/MOU.

Mail Claims Packet to address shown on upper left corner of DPSS 2076A.
[see method, time, and schedule/condition of payments).
(Please type or print information on all DPSS Forms.)

DPSS 2076A
CONTRACTOR PAYMENT REQUEST

"Remit to Name"
The legal name of your agency.

"Address" “City, State, and Zip Code”
The remit to address used when this contract was established for your agency. All address changes must be submitted for processing prior to use.

"Contract Number"
Can be found on the first page of your contract.

"Amount Requested"
Fill in the total amount and billing period you are requesting payment for.

"Payment Type"
Check the box and enter the dollar amount for the type(s) of payment(s) you are requesting payment for.

"Any questions regarding…"
Fill in the name and phone number of the person to be contacted should any questions arise regarding your request for payment.

EVERYTHING BELOW THE THICK SOLID LINE IS FOR DPSS USE ONLY AND SHOULD BE LEFT BLANK.

COUNTY OF RIVERSIDE DEPARTMENT OF PUBLIC SOCIAL SERVICES CONTRACTOR EXPENDITURE REPORT (2076B)	
CONTRACTOR:	
ACTUAL EXPENDITURES FOR (MM/YYYY)	
CONTRACT #:	

EXPENSE CATEGORY	APPROVED BUDGETED AMOUNT	CURRENT EXPENDITURES BILLABLE AMOUNT	CUMULATIVE EXPENDITURES	UNEXPENDED BUDGETED AMOUNT
List each item as outlined in contract budget.				
TOTAL BUDGET/EXPENSES				

IN-KIND CASH CONTRIBUTION

List each type of contribution				
TOTAL IN-KIND/CASH MATCH				

CLIENT FEES COLLECTED	CURRENT PERIOD	YEAR TO DATE

Attachment V
JUMP Technology Services, L.L.C.
Enterprise Subscription Agreement (Order Form)

JUMP TECHNOLOGY SERVICES, LLC. ENTERPRISE SUBSCRIPTION AGREEMENT

AGREEMENT #: _____

EFFECTIVE DATE: _____

EXPIRATION DATE: _____

This agreement is made between JUMP Technology Services, L.L.C. (hereafter referred to as JUMP Technology Services) and Riverside County Department of Public Social Services (hereafter referred to as Customer) and will become effective upon execution and will continue in effect until the services provided for herein have been performed or until terminated as provided herein. Each of JUMP Technology Services and Customer may be referred to herein individually as a “Party” and together as the “Parties.” This Agreement, including the Schedules, supersedes all prior proposals, negotiations, and communications, oral or written, between the parties with respect to the subject matter hereof; no modification or amendment to this Agreement shall be binding unless in writing and signed by representatives of both parties. This Agreement may be executed in any number of counterparts, each of which shall be an original, and such counterparts together shall constitute one and the same instrument. Execution may be affected by delivery of email or facsimile of signature pages, which shall be deemed originals in all respects.

All Customer orders must be made by properly submitting completed Schedules signed by Customer and JUMP. All Schedules shall refer to this Agreement by number and will incorporate the terms of this Agreement.

The term of this agreement shall be from 07/01/2026 through 06/30/2031. The maximum amount of this contract shall not exceed $972,319.20.

Schedules

_____Schedule A: Definitions
_____Schedule B: Service Level Agreement
_____Schedule C: Training
_____Schedule D: Statement of Services

1 DEFINITIONS

Bolded terms used herein but not defined, have the meaning set forth in Schedule A.

2 LICENSED SOFTWARE

2.1 CUSTOMER will receive a personal, nonexclusive, and nontransferable license to use the Licensed Software and related documentation during the term designated on this Agreement.

2.2 Except for the rights expressly granted herein, this Agreement does not transfer from JUMP Technology Services to CUSTOMER any intellectual property and/or developed technology, and all right, title, and interest in and to such property/technology will remain solely with JUMP Technology Services. CUSTOMER shall supervise and approve access for all Authorized Users of the Licensed Software and shall prevent unauthorized access and use of the Licensed Software. CUSTOMER may not use any component of the System to provide services to third parties as a service bureau or data processor.

3 SERVICES

This Agreement sets forth the terms and conditions under which JUMP Technology Services agrees to provide (i) certain hosted “software as a service” (“Subscription Services”) for certain software applications (each such application together with any applicable documentation thereto, and programming and user interfaces therefore, a “Platform”) to Authorized Users, as further set forth on each order form (“Order Form”) and (ii) if applicable, all other implementation services, customization, integration, data import and export, monitoring, technical support, maintenance, training, backup and recovery, and change management (“Professional Services” together with Subscription Services, the “Services”) related to CUSTOMER’s access to, and use of, such Subscription Services and each Platform, as further set forth on each statement of services (“Statement of Work”) issued hereunder (Order Forms and Statements of Professional Services are sometimes referred to jointly as a “Statement of Services”).

3.1 Platform. During the term set forth in this Agreement, JUMP Technology Services shall provide CUSTOMER (a) a non-exclusive, non-assignable, limited right to access and use the Platform during the Term, solely for CUSTOMER’s internal business operations and subject to the terms of this Agreement and schedules; and (b) Software support as set forth in Schedule D.

3.2 Subscription Services. Each applicable Order Form shall specify and further describe the Subscription Services to be provided in accordance with the representations and warranties set forth herein, and shall identify, each applicable Platform, user limitations, fees, subscription term and other applicable terms and conditions. For Licensed Software, JUMP Technology Services shall provide the Support Services as set forth in Schedule D.

3.3. Professional Services. Unless otherwise stated, Professional Services shall be performed on a time and materials basis at JUMP’s standard rates.

3.4 Changes to Platform. JUMP Technology Services may, in its sole discretion, make any changes to any Platform that it deems necessary or useful to maintain or enhance (a) the quality or delivery of JUMP Technology Services’ products or services to its CUSTOMERs, (b) the competitive strength of, or market for, JUMP Technology Services’ products or services, (c) such Platform’s cost efficiency or performance, or (ii) to comply with applicable law.

3.5 CUSTOMER Responsibilities. CUSTOMER shall approve access for all Authorized Users to the Platform and shall prevent unauthorized access and use of the Platform and licensed software. CUSTOMER shall not and shall ensure that its Authorized Users do not: (i) sell, resell, lease, lend or otherwise make available the licensed software to a third-party; (ii) modify, adapt, translate, or make derivative works of the licensed software; or (iii) sublicense or operate the licensed software for timesharing, outsourcing, or service bureau operations. CUSTOMER will maintain sufficient bandwidth and network connectivity for the operation of the licensed software and subscription services and shall have sole responsibility for installation, testing, and operations of CUSTOMER facilities, telecommunications and internet services, equipment, and software upon CUSTOMER’s premises necessary for CUSTOMER’s use of the licensed software. CUSTOMER will pay all third-party access fees incurred by CUSTOMER to access and use the Platform and licensed software.

4 PLATFORM ACCESS AND AUTHORIZED USER

4.1 Administrative Users. During the configuration and set-up process for each Platform, CUSTOMER will identify an initial administrative user account which will be configured by JUMP Technology Services account during initial implementation. CUSTOMER will be responsible for creating CUSTOMER’s additional administrative accounts. JUMP Technology Services will maintain its administrative accounts to assist CUSTOMER in support of its service level agreement.

4.2 Authorized Users. CUSTOMER may allow such a number of CUSTOMER’s employees and/or independent contractors as is indicated on Schedule D to use the applicable Platform on behalf of CUSTOMER as “Authorized Users.” Authorized User subscriptions are for designated Authorized Users and cannot be shared or used by more than one Authorized User. Newly Authorized Users must have their own account and unique email address. CUSTOMER will be responsible for monitoring active licensed users and inactive accounts that should no longer have access to the Platform.

CUSTOMER will be responsible for requesting the next license level to add more licenses to this Agreement as needed. JUMP Technology Services audits licensed users monthly and will notify CUSTOMER via the CUSTOMER Portal if CUSTOMER exceeds their contracted license limit. If CUSTOMER does not right the overage within 30 business days, JUMP Technology Services will send an invoice for the additional licenses that are being used.

4.3 Authorized User Conditions to Use. As a condition to access and use of a Platform each Authorized User shall agree to abide by the terms of use laid out in this Agreement.

4.4. Account Responsibility. CUSTOMER will be responsible for (i) all uses of any account created by CUSTOMER or created by JUMP Technology Services at CUSTOMER's written request, regardless of CUSTOMER's knowledge of such use, and (ii) securing its passwords (including but not limited to administrative and user passwords) and files. JUMP Technology Services is not responsible for any losses, damages, costs, expenses or claims that result from stolen or lost passwords of CUSTOMER user accounts. CUSTOMER shall also ensure that each Authorized User uses their own unique login and password when they log into the Platform.

5 ADDITIONAL RESTRICTIONS AND RESPONSIBILITIES

5.1 Software Restrictions. CUSTOMER will not, nor permit or encourage any third party to, directly or indirectly (i) reverse engineer, decompile, deconstruct or otherwise attempt to discover or derive the source code, object code or underlying structure, ideas, know-how or algorithms relevant to the Platform, Software (ii) modify, translate, or create derivative works based on a Platform or any Software; (iii) use a Platform or any Software for timesharing or service bureau purposes or other computer service to a third party; (iv) modify, remove or obstruct any proprietary notices or labels; or (v) use any Software or a Platform in any manner to assist or take part in the development, marketing or sale of a product potentially competitive with such Software or Platform. Software and the Services are the Confidential Information of JUMP Technology Services.

5.2 CUSTOMER Compliance. CUSTOMER shall use, and will ensure that all Authorized Users use, each Platform, Software, and the Services in full compliance with this Agreement and all applicable laws and regulations. CUSTOMER represents and warrants that it (i) has accessed and reviewed any terms of use or other policies relating to the Platform and licensed software provided by JUMP Technology Services, (ii) understands the requirements thereof, and (iii) agrees to comply therewith. JUMP Technology Services may suspend CUSTOMER's account and access to each Platform and Services at any time and without notice if JUMP Technology Services reasonably believes that CUSTOMER is in violation of this Agreement. Although JUMP Technology Services has no obligation to monitor CUSTOMER's use of a Platform, JUMP Technology Services may do so and may prohibit any use it believes may be (or alleged to be) in violation of the foregoing.

5.3 Cooperation. CUSTOMER shall provide all cooperation and assistance as JUMP Technology Services may reasonably request to enable JUMP Technology Services to exercise its rights and perform its obligations under, and in connection with, this Agreement, including providing JUMP Technology Services with such access to CUSTOMER's premises and its information technology infrastructure as is necessary for JUMP Technology Services to perform the Services in accordance with this Agreement.

5.4 Training and Education. CUSTOMER shall use commercially reasonable efforts to cause Authorized Users to be, at all times, educated and trained in the proper use and operation of each Platform that such Authorized Users utilize, and to ensure that each Platform is used in accordance with applicable manuals, instructions, specifications, and documentation provided by JUMP Technology Services. CUSTOMER shall be responsible for entering a help desk ticket when one-on-one new user training is needed.

5.5. CUSTOMER Systems. CUSTOMER shall be responsible for obtaining and maintaining—both the functionality and security of—any equipment and ancillary services needed to connect to, access or otherwise use each Platform, including modems, hardware, servers, software, operating systems, networking, web servers and the like.

5.6 Restrictions on Export. CUSTOMER shall not to transfer, or authorize the transfer of, the Licensed Software to a prohibited country or otherwise in violation of any such restrictions or regulations.

6 CONFIDENTIALITY

6.1 Confidential Information. With respect to Confidential Information of the Disclosing Party, the Receiving Party agrees to: (i) use the same degree of care to protect the confidentiality, and prevent the unauthorized use or disclosure, of such Confidential Information, that it uses to protect its own proprietary and confidential information of like nature, which shall not be less than a reasonable degree of care, (ii) hold all such Confidential Information in strict confidence and not use, sell, copy, transfer reproduce, or divulge such Confidential Information to any third party, (iii) not use such Confidential Information for any purposes whatsoever other than the performance of, or as otherwise authorized by, this Agreement.

6.2 Compelled Disclosure. The Receiving Party may disclose Confidential Information of the Disclosing Party to the extent necessary to comply with a court order or applicable law, including but not limited to California Public Records Act and California Brown Act; provided, however that the Receiving Party delivers reasonable advance notice of such disclosure to the Disclosing Party and uses reasonable efforts to secure confidential treatment of such Confidential Information, in whole or in part.

6.3 Remedies for Breach of Obligation of Confidentiality. The Receiving Party acknowledges that breach of its obligation of confidentiality may cause irreparable harm to the Disclosing Party for which the Disclosing Party may not be fully or adequately compensated by recovery of monetary damages. Accordingly, in the event of any violation, or threatened violation, by the Receiving Party of its obligations under this Section, the Disclosing Party shall be entitled to seek injunctive relief from a court of competent jurisdiction in addition to any other remedy that may be available at law or in equity, without the necessity of posting bond or proving actual damages. Disclosing Party has the right to terminate this Agreement upon discovery of such breach.

7 PROPRIETARY RIGHTS

7.1 Ownership. CUSTOMER shall own all right, title, and interest in and to the **CUSTOMER Data.** JUMP Technology Services shall own and retain all right, title, and interest in and to (i) each Platform, Software and the Services and all improvements, enhancements, test scripts, documents, or modifications thereto, (ii) any software, applications, inventions, or other technology developed in connection with the Services, and (iii) all intellectual property and proprietary rights in and related to any of the foregoing. JUMP Technology Services shall grant to CUSTOMER a non-exclusive, non-transferable license to use the **Platform** only for CUSTOMER's own internal purposes in connection with the Licensed Software and Services.

7.2 CUSTOMER Data and Vendor Information License. CUSTOMER hereby grants to JUMP Technology Services a non-exclusive, transferable, sublicensable, worldwide and royalty-free license to use and otherwise exploit (i) **CUSTOMER Data** to provide the Services to CUSTOMER hereunder and as necessary or useful to monitor and improve a Platform, Software, and the Services, both during and after the Term. For the avoidance of doubt, JUMP Technology Services may use, reproduce, and disclose **Platform-, Software-** and Services-related information, data and material that is anonymized, de- identified, or otherwise rendered not reasonably associated or linked to CUSTOMER or any other identifiable individual person or entity for product improvement and other lawful purposes, all of which information, data and material will be owned by JUMP Technology Services. CUSTOMER acknowledges that it will not have access to CUSTOMER Data through JUMP Technology Services or any Platform following the expiration or termination of this Agreement except as provided in Section 9.4.

7.3 Aggregated Statistical Information. JUMP Technology Services owns the aggregated and statistical data derived from the operation of the **Platform**, including, without limitation, the number of records created by the **Platform**, the numbers and types of transactions, configurations, and reports processed and the performance results ("Aggregated Statistical Information"). Nothing in this agreement shall be construed as prohibiting JUMP Technology Services from utilizing the Aggregated Statistical Information for purposes of providing or improving its services, bench marking service performance, preparing statistics and system metrics, and marketing; provided however, that JUMP Technology Services' use of Aggregated Statistical Information does not disclose any information that is related to an identified or identifiable individual and has been provided by CUSTOMER within the Platform **("CUSTOMER Data")** to any third party.

7.4 No Other Rights. No rights or licenses are granted except as expressly set forth herein.

8 FEES & PAYMENT

8.1 Fees. CUSTOMER shall pay all fees set forth herein and laid out in Schedule D.
Payment. JUMP Technology Services may choose to bill through an invoice, in which case, full payment for invoices issued in any given month must be received by JUMP Technology Services within forty-five (45) calendar days of receipt of invoice.

Invoices shall be sent to:
Department of Public Social Services
Fiscal/Management Reporting Unit
4060 County Circle Drive
Riverside, CA 92503
OperationgServicesContractPayments@rivco.org

Payments shall be made to:
JUMP Technology Services, L.L.C.
P.O. Box 3452
Edmond, OK 473083

8.3 Payment Disputes. If CUSTOMER believes that JUMP Technology Services has billed CUSTOMER incorrectly, CUSTOMER must contact JUMP Technology Services no later than forty-five (45) days after the mailing date of the invoice, or received date if sent electronically, in order to receive an adjustment or credit. Inquiries should be directed to JUMP Technology Services' CUSTOMER support department or the applicable Account Manager.

8.4 No Deductions or Setoffs. All amounts payable to JUMP Technology Services hereunder shall be paid by CUSTOMER to JUMP Technology Services in full without any setoff, recoupment, counterclaim, deduction, debit or withholding for any reason except as may be required by applicable law.

8.5 License Overage. JUMP Technology Services reserves the right to audit CUSTOMER's use of the Platform. If CUSTOMER's use is greater than contracted, CUSTOMER shall be invoiced for any licenses used above the amount set forth herein. If any increase in fees is required, CUSTOMER shall also pay the expenses associated with the audit.

8.6 Taxes. CUSTOMER shall pay all shipping charges, as well as any taxes, fees or costs imposed by any governmental body arising as a result of this Agreement. JUMP Technology Services shall be responsible for taxes on its net income.

9 TERM AND TERMINATION

9.1 Term. This Agreement shall remain in effect until its termination as provided below (the "Term"). The term of each Statement of Services shall begin on the applicable "Services Effective Date" and continue until all Services expire or are terminated in accordance with this Agreement.

9.2 Termination. JUMP Technology Services may terminate this Agreement upon written notice to CUSTOMER if no Statement of Services is in effect. In addition to any other remedies it may have, either party may also terminate this Agreement upon written notice if the other party fails to pay any amount when due or otherwise materially breaches this Agreement and fails to cure such breach within thirty (30) days or as agreed upon by both parties after receipt of written notice of such breach from the non-breaching party. Notwithstanding the foregoing, if CUSTOMER is a state agency or a political subdivision of a state, or a federal agency or a political subdivision of the federal government, CUSTOMER may terminate this Agreement at any time (i) for convenience upon ninety (90) days' written notice to JUMP Technology Services, or (ii) if adequate funds to pay JUMP Technology Services all fees owed hereunder are not appropriated to such CUSTOMER during the Term, unless otherwise authorized by law; provided, it is expressly agreed that CUSTOMER shall not activate this non-appropriation provision for its convenience, substation for another procurement system or solution, or to circumvent the requirements of this Agreement in any way. Furthermore, failure to use the Licensed Software, Services, and Platform or Upgrades thereto in accordance with Applicable Law is a material breach of this Agreement and cause for termination.

9.3 Effect of Termination. Upon termination of the Agreement, each outstanding Statement of Services, if any, shall terminate and CUSTOMER shall immediately cease all use of, and all access to, the Subscription Services and JUMP Technology Services shall immediately cease providing the Professional Services. If (i) JUMP Technology Services terminates this Agreement pursuant to the second sentence of Section 9.2, or (ii) CUSTOMER terminates this Agreement pursuant to clause (ii) of Section 9.2, all Fees that would have become payable had each outstanding Statement of Service remained in effect until expiration of its current term will become immediately due and payable.

9.4 CUSTOMER Data Upon Termination. Upon termination of the Agreement, all CUSTOMER Data retained by JUMP Technology Services in database files shall be made available to CUSTOMER by a SQL Server database backup file (.bak) for a period of 60 days after the termination of this Agreement. Thereafter, JUMP Technology Services shall securely destroy CUSTOMER Data using a method that prevents recovery of the data in accordance with industry best practices for

wiping of electronic media (e.g. NIST SP 800-88r1). All CUSTOMER Data will be rendered unreadable and unrecoverable.

9.5 Survival. Sections [3.1, 7.2, 7.4, and 9.4] shall survive any termination or expiration of this Agreement. All other rights and obligations shall be of no further force or effect.

10 WARRANTY AND DISCLAIMER

10.1 Warranties. JUMP Technology Services represents and warrants that it will perform the Professional Services in a professional and workmanlike manner. Each party represents and warrants that it has the legal power to enter into this Agreement. Additionally, CUSTOMER warrants that (i) CUSTOMER owns or has a license to use and has obtained all consents and approvals necessary for the provision and use of all of the CUSTOMER Data that is placed on, transmitted via or recorded by a Platform and the Services; (ii) the provision and use of CUSTOMER Data as contemplated by this Agreement and each Platform and the Services does not and shall not violate any CUSTOMER's privacy policy, terms- of-use or other agreement to which CUSTOMER is a party or any law or regulation to which CUSTOMER is subject to; and (iii) with the exception of social security numbers, no CUSTOMER Data will include bank routing numbers, credit card or debit card numbers, credit report information or other information that is subject to international, federal, state, or local laws or ordinances now or hereafter enacted regarding data protection or privacy, including, but not limited to, the Fair Credit Reporting Act, and the Gramm-Leach-Bliley Act. Additionally, CUSTOMER warrants that it will not enter data governed by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) unless JUMP Technology Services has indicated in writing in Schedule D – Statement of Services that the system provided by JUMP Technology Services is offered for the purposes of collecting protected health information.

10.2 Remedy. CUSTOMER's sole and exclusive remedy for any breach of the warranties set forth herein or in an Order Form shall be to notify JUMP Technology Services of the applicable non-conformity, in which case JUMP Technology Services shall use commercially reasonable efforts to correct such non-conformity. Notwithstanding the foregoing, JUMP Technology Services shall not be responsible for any non-conformity which arises as a result of (a) any act or omission of CUSTOMER, including a failure to use the System or Services in conformance with the Documentation or Applicable Law; (b) any person (other than JUMP Technology Services) making modifications to the Platform in any way without JUMP Technology Services' prior written consent; or (c) any failure of any component of Hardware, Sublicensed Software, or any CUSTOMER-supplied software, equipment, or other third-party materials.

10.3 No Virus Warranty. JUMP Technology Services warrants that it will provide the Services free of viruses, worms, time bombs, Trojan horses, corrupted files, or other computer programming routines that are intended to damage, detrimentally interfere with, surreptitiously intercept, or expropriate any systems, data, personal information, or property of another ("Malicious Code"). This warranty does not extend to CUSTOMER media files.

10.4 Security, Data and Backup Warranty. JUMP Technology Services warrants that JUMP Technology Services will use commercially reasonable efforts to safeguard and accurately maintain CUSTOMER Data, consistent with industry security standards and backup procedures. In the event of a breach, JUMP Technology Services shall use commercially reasonable efforts to correct CUSTOMER Data or restore CUSTOMER Data as quickly as possible, but in any case not to exceed three (3) business days. This warranty does not extend to any Third-Party Applications or CUSTOMER Data not hosted by JUMP Technology Services.

10.5 Warranty of Title. JUMP Technology Services warrants that it is the owner of the Platform or otherwise has the right to provide the Services as set forth in this Agreement without violating any proprietary rights of any third parties.

10.6 Disclaimer. EXCEPT AS EXPRESSLY PROVIDED HEREIN OR IN A STATEMENT OF SERVICE, JUMP TECHNOLOGY SERVICES DOES NOT WARRANT THAT ACCESS TO THE PLATFORMS, SOFTWARE OR SERVICES WILL BE UNINTERRUPTED OR ERROR FREE, NOR DOES JUMP TECHNOLOGY SERVICES MAKE ANY WARRANTY AS TO THE RESULTS THAT MAY BE OBTAINED FROM USE OF THE SERVICES. FURTHER, JUMP TECHNOLOGY SERVICES MAKES NO REPRESENTATIONS OR WARRANTIES WITH RESPECT TO SERVICES PROVIDED BY THIRD PARTY TECHNOLOGY SERVICE PROVIDERS RELATING TO OR SUPPORTING A PLATFORM, INCLUDING HOSTING AND MAINTENANCE SERVICES, AND ANY CLAIM OF CUSTOMER ARISING FROM OR RELATING TO SUCH SERVICES SHALL, AS BETWEEN JUMP TECHNOLOGY SERVICES AND SUCH SERVICE PROVIDER, BE SOLELY AGAINST SUCH SERVICE PROVIDER. THE PLATFORMS, SOFTWARE AND SERVICES ARE PROVIDED "AS IS," AND JUMP TECHNOLOGY SERVICES DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW.

10.7 CUSTOMER Warranty. CUSTOMER warrants that CUSTOMER (a) has the power and authority to enter into this Agreement, and CUSTOMER shall be responsible for all acts and omissions of all CUSTOMER affiliates and Authorized Users; and (b) shall use its best efforts to protect the security of the Licensed Software and Services.

10.8 Remedies for Malicious Code. In addition to Vendor's obligation to use commercially reasonable efforts to correct any non conformity, upon discovery

or notification of Malicious Code introduced, enabled, or propagated by Vendor Systems or Services, Vendor shall: (a) begin containment within 4 hours, and use best efforts to eradicate within 24 hours with complete full remediation within 72 hours; (b) restore affected data, configurations, and services to their pre incident state; (c) reimburse Customer's reasonable, documented costs for incident response, forensics, restoration, re imaging, and necessary security hardening; (d) defend, indemnify, and hold harmless Customer from third party claims and losses arising out of such Malicious Code. The foregoing obligations shall not be limited by any liability caps or exclusions for indirect or consequential damages to the extent such losses consist of investigation, remediation, restoration, and third party claim defense costs. Repeated incidents or failure to remediate within SLA timelines shall entitle Customer to terminate for cause with prorated refunds and transition assistance.

10.9 Security, Data, and Backup Remedies. Vendor warrants that Customer Data will be safeguarded and backed up in accordance with industry standard security controls, including encryption in transit and at rest, and successful periodic restore tests. Vendor shall: (a) notify Customer within 24 hours of any Security Incident affecting Customer Data; (b) cooperate with Customer in regulatory notifications and investigations; (c) reimburse reasonable, documented costs for data restoration, re entry, and reconstruction where backups are unavailable or corrupted; and (d) defend and indemnify Customer for third party claims and direct breach response costs, including forensic investigation, notification, and regulatory assessments to the extent permitted by law. The obligations in this Section are carved out from any liability caps and damages exclusions.

11 INDEMNITY

Reserved.

12 LIMITATION OF LIABILITY

12.1 IN NO EVENT SHALL (I) EITHER PARTY'S LIABILITY ARISING OUT OF OR RELATED TO THIS AGREEMENT, WHETHER IN CONTRACT, TORT OR UNDER ANY OTHER THEORY OF LIABILITY EXCEED IN THE AGGREGATE TWO (2) TIMES E THE TOTAL FEES PAID OR OWED BY CUSTOMER AND VENDORS HEREUNDER DURING THE FOURTY EIGHT (48) MONTHS IMMEDIATELY PRECEDING THE DATE OF THE EVENT GIVING RISE TO THE CLAIM (SUCH AMOUNT BEING INTENDED AS A CUMULATIVE CAP AND NOT PER INCIDENT), PROVIDED, HOWEVER, THAT FOR CLAIMS ARISING FROM (A) BREACH OF CONFIDENTIALITY, (B) DATA BREACH, SECURITY INCIDENT, OR LOSS, CORRUPTION, OR UNAUTHORIZED DISCLOSURE OF CUSTOMER DATA, (C) VENDOR'S INTRODUCTION OR PROPAGATION OF MALICIOUS CODE, (D) VENDOR'S OBLIGATIONS TO RESTORE, RECREATE, OR CORRECT CUSTOMER DATA, OR (E) VENDOR'S INDEMNIFICATION OBLIGATIONS, VENDOR'S AGGREGATE LIABILITY SHALL BE INCREASED TO THE GREATER OF (1) FIVE (5) TIMES THE TOTAL FEES PAID OR OWED BY CUSTOMER TO VENDOR IN THE TWELVE (12) MONTHS PRIOR TO THE EVENT GIVING RISE TO THE CLAIM, OR (2) $2,000,000.AND (II) EITHER PARTY HAVE ANY LIABILITY TO THE OTHER FOR ANY LOST PROFITS OR REVENUES OR FOR ANY INDIRECT, INCIDENTAL, CONSEQUENTIAL, COVER, SPECIAL, EXEMPLARY OR PUNITIVE DAMAGES, HOWEVER CAUSED, WHETHER IN CONTRACT, TORT OR UNDER ANY OTHER THEORY OF LIABILITY, AND WHETHER OR NOT THE PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. EXCEPT THAT THE FOREGOING EXCLUSION SHALL NOT APPLY TO DAMAGES ARISING FROM (A) BREACH OF CONFIDENTIALITY, (B) DATA BREACH, SECURITY INCIDENT, OR LOSS OR CORRUPTION OF CUSTOMER DATA, (C) VENDOR'S INDEMNIFICATION OBLIGATIONS, (D) VENDOR'S GROSS NEGLIGENCE OR WILLFUL MISCONDUCT, OR (E) VENDOR'S INTRODUCTION OF MALICIOUS CODE.

THE FOREGOING LIMITATIONS AND DISCLAIMERS SHALL NOT APPLY TO THE EXTENT PROHIBITED BY APPLICABLE LAW.

NOTHING IN THIS SECTION LIMITS CUSTOMER'S RIGHTS OR REMEDIES UNDER APPLICABLE LAW GOVERNING CALIFORNIA COUNTIES.

12.2 Limitation on Actions..Reserved.

13 GOVERNING LAW AND DISPUTE RESOLUTION

Reserved.

14 SECURITY

14.1 Data Center Procedures. JUMP Technology Services maintains the Platform using a third-party service provider authorized by the Federal Risk and

Authorization Management Program ("FedRAMP"). CUSTOMER acknowledges that JUMP Technology Services cannot offer any additional or modified procedures other than those put in place by such technology provider.

14.2 Remediation of Certain Unauthorized Disclosures. In the event that any unauthorized access to or acquisition of CUSTOMER Data is caused by JUMP Technology Services' breach of its security and/or privacy obligations under this Agreement, JUMP Technology Services shall provide CUSTOMER notification as required by Law and pay the reasonable and documented costs CUSTOMER incurs in connection with the following items: (a) costs of any required forensic investigation to determine the cause of the breach, (b) providing notification of the security breach to applicable government and relevant industry self-regulatory agencies, to the media (if required by Law) and to individuals whose Personal Data may have been accessed or acquired, (c) providing credit monitoring service to individuals whose Personal Data may have been accessed or acquired for a period of one year after the data on which such individuals were notified of the unauthorized access or acquisition for such individuals who elected such credit monitoring service, and (d) operating a call center to respond to questions from individuals whose Personal Data may have been accessed or acquired for a period of one year after the data on which such individuals were notified of the unauthorized access or acquisition. NOTWITHSTANDING THE FOREGOING, OR ANYTHING IN THE AGREEMENT TO THE CONTRARY, JUMP TECHNOLOGY SERVICES SHALL HAVE NO RESPONSIBILITY TO PAY COSTS OF REMEDIATION THAT ARE DUE TO RECKLESS MISCONDUCT, GROSS NEGLIGENCE, WILLFUL MISCONDUCT AND/OR FRAUD BY CUSTOMER OR CUSTOMER USERS, AGENTS OR CONTRACTORS.

15 PUBLICITY

15.1 CUSTOMER agrees that JUMP Technology Services may identify CUSTOMER as a CUSTOMER in JUMP Technology Services's promotional materials. CUSTOMER may request that JUMP Technology Services stop doing so by submitting an email to solutions@jumpfaster.com at any time . CUSTOMER acknowledges that it may take JUMP Technology Services up to 30 days to process such request. Notwithstanding anything herein to the contrary, CUSTOMER acknowledges that JUMP Technology Services may disclose the existence and terms and conditions of this Agreement to its advisors, actual and potential sources of financing, and to third parties for purposes of due diligence.

16 NOTICES

16.1 All notices, consents, and other communications between the parties under or regarding this Agreement must be in writing (which includes email and facsimile) and be addressed according to information provided on an Order Form in the Statement of Services. All communications will be deemed to have been received on the date actually received. Either party may change its address for notices by giving written notice of the new address to the other party in accordance with this Section.

17 FORCE MAJEURE

17.1 JUMP Technology Services is not responsible nor liable for any delays or failures in performance from any cause beyond its control, including, but not limited to acts of God, changes to law or regulations, embargoes, war, terrorist acts, acts or omissions of third party technology providers, riots, fires, earthquakes, floods, power blackouts, strikes, weather conditions or acts of hackers, internet service providers or any other third party or acts or omissions of CUSTOMER or any Authorized User.

18 ASSIGNMENT

18.1 Neither Party shall assign its rights, duties or obligations under this Agreement without the prior written consent of the other Party and such consent shall not be unreasonably withheld. Notwithstanding the foregoing, JUMP Technology Services may assign this Agreement to an affiliate or in connection with any merger, reorganization or sale of substantially all of JUMP Technology Services' assets without any consent from CUSTOMER. For the avoidance of doubt, a third-party technology provider that provides features or functionality in connection with a Platform shall not be deemed a sublicensee under this Agreement.

19 RELATIONSHIP OF THE PARTIES

19.1 The relationship between CUSTOMER and JUMP Technology Services created under this Agreement shall be that of independent contractors.

20 GENERAL PROVISIONS

20.1 If any provision of this Agreement is found to be unenforceable or invalid, that provision will be limited or eliminated to the minimum extent necessary so that this Agreement will otherwise remain in full force and effect and enforceable. This Agreement, together with Statement of Services entered into hereunder and all schedules, annexes and addenda hereto and thereto is the complete and exclusive statement of the mutual understanding of the parties and supersedes and cancels

all previous written and oral agreements, communications and other understandings relating to the subject matter of this Agreement. All waivers and modifications must be in writing signed by both parties, except as otherwise provided herein. No agency, partnership, joint venture, or employment is created as a result of this Agreement, and neither party has authority of any kind to bind the other party in any respect whatsoever. In the event of a conflict between this Agreement and any Statement of Services, such Statement of Services shall prevail (unless otherwise expressly indicated in this Agreement or such Statement of Services), and the enforceability of the remaining provisions shall not be impaired. The heading references herein are for convenience purposes only and shall not be deemed to limit or affect any of the provisions hereof. Unless otherwise indicated to the contrary herein by the context or use thereof: (i) the words “hereof,” “hereby,” “herein,” “hereto,” and “hereunder” and words of similar import shall refer to this Agreement as a whole and not to any particular Section or paragraph of this Agreement; (ii) the words “include,” “includes” or “including” are deemed to be followed by the words “without limitation;” (iii) references to a “Section” or “Exhibit” are references to a section of, or exhibit to this Agreement; and (iv) derivative forms of defined terms will have correlative meanings.

20.2 Purchase Orders and Acceptance of Quotes:. If CUSTOMER submits its own terms which add to, vary from, or conflict with the terms herein in CUSTOMER’s acceptance of a price quote or in a purchase order, or to JUMP Technology Services’ employees and/or agents in the course of JUMP Technology Services providing the Licensed Software and/or Services, any such terms are of no force and effect and are superseded by this Agreement.

20.3 Non-Solicitation. During the term of this Agreement and for a period of one (1) year thereafter, CUSTOMER agrees not to hire, directly or indirectly, any employee or former employee of JUMP Technology Services, without obtaining JUMP Technology Services’ prior written consent.

20.4 California Consumer Privacy Act. The Parties agree that the California Consumer Privacy Act under Cal. Civ. Code § 1798 et seq. (“CCPA”) may be applicable to the Agreement. If applicable, JUMP Technology Services shall be deemed a “service provider” under the CCPA if JUMP Technology Services receives the "personal information" of any “consumer” for "processing" on CUSTOMER’s behalf.

Schedule A: Definitions

Authorized Users means a user that has been permitted to use the Licensed Software, Sublicensed Software, Services, and/or Platform as described in the applicable Order Form.

Change Order means a written agreement signed by JUMP Technology Services and CUSTOMER stating their agreement upon all of the following: (1) a change in the Services; (2) the amount of the adjustment in the Contract Total, if any, and (3) the extent of the adjustment in the Term, if any.

Confidential Information means (i) the source and object code of all components of the System, (ii) the Documentation, (iii) the Test Scripts, (iv) the design and architecture of the database, (v) all other information of a confidential or proprietary nature disclosed by one Party to the other Party in connection with this Agreement which is either (x) disclosed in writing and clearly marked as confidential at the time of disclosure or (y) disclosed orally and clearly designated as confidential in a written communication to the receiving Party within 7 days following the disclosure. “Confidential Information” shall not include information (a) publicly available through no breach of this Agreement, (b) independently developed or previously known to it, without restriction, prior to disclosure by the disclosing Party, (c) rightfully acquired from a third-party not under an obligation of confidentiality.

CUSTOMER Data shall mean all electronic data or information submitted by CUSTOMER to the Licensed Software or Services but excluding Deidentified Data (as defined below).

“De-identified Data” means CUSTOMER Data that is de-identified by JUMP Technology Services and such de-identification is certified by a third-party as compliant with the de-identification standards under HIPAA or otherwise meets the de-identification requirements under HIPAA.

Federal Risk and Authorization Management Program (“FedRAMP”) is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. More information can be found at https://www.fedramp.gov/ FedRAMP supports agencies and cloud service providers through the FedRAMP authorization process and maintains a secure repository of FedRAMP authorizations to enable reuse of security packages.

Order Form means a work authorization executed by the Parties from time to time laying out the items being purchased by the CUSTOMER, scope of use, pricing, payment terms and any other relevant terms, which will be a part of and be governed by the terms and conditions of this Agreement.

Platform shall mean the Software delivered under the Subscription Services which includes supporting software, and programming, and user interfaces to Authorized

Users as set forth in an Order Form.

Professional Services means, collectively, the implementation, installation, data conversion, consultation, and training services provided by JUMP Technology Services under or in connection with this Agreement.

Service Level Agreement shall mean the contractually binding agreement between JUMP Technology Services and the CUSTOMER regarding types and standard of services to be provided.

Services shall mean the Professional Services and the Subscription Services set forth in an Order Form.

Licensed Software shall mean the program specific Software as a Service to which the CUSTOMER is subscribing with individual licensed user accounts as set forth in an Order Form.

Subscription Services shall mean the services to keep the Licensed Software in working order and to sustain useful life of the Licensed Software, including Updates and specified in an Order Form.

Software means the object code version of computer programs developed by JUMP Technology Services and listed on an Order Form, including Updates furnished to CUSTOMER by JUMP Technology Services pursuant to this Agreement or any Order Form, but excluding all Sublicensed Software or third party software.

Schedule B: Service Level Agreement

1.0 Support is provided under an annual contract that provides CUSTOMER access to a dedicated support team during normal business hours. Normal business hours are between 5 a.m. and 5:00 p.m. (CUSTOMER' Local Time), Monday through Friday, excluding national and JUMP company holidays. A list of JUMP company holidays is below as 8.0 JUMP Technology Services Company Holidays and is subject to change from year to year. The total number of JUMP company holidays is not to exceed ten (10) days per year. The Support Services Center (“SSC”) web site address is https://jumpssc.com. The customer portal will be accessible 24 hours a day.

After hours emergency support will be via emergency phone numbers provided to CUSTOMER for reporting the unavailability of services or platform components where maintenance has not been scheduled and previously announced to CUSTOMER via maintenance notifications through the SSC.

2.0 Periodically, JUMP Technology Services will require Scheduled Downtime, for updates and system upgrades. Scheduled Downtime will normally be scheduled outside of normal business hours, with twenty-four (24) hours’ notice, or in the event of a more urgent need JUMP Technology Services may give less notice to resolve an immediate security need. It is anticipated that there will be monthly scheduled downtime for system maintenance, JUMP Technology Services will post all downtime announcements on the customer portal.

CUSTOMER acknowledges and agrees that, from time to time, the Platform may be inaccessible or inoperable for the following reasons: (i) equipment malfunctions; (ii) periodic maintenance; or (iii) catastrophic events beyond the control of JUMP Technology Services or that are not reasonably foreseeable by JUMP Technology Services. Client shall report any Unscheduled Downtime by calling JUMP Technology Services with the provided support number within one (1) day of its occurrence.

The performance and availability of the Platform are directly dependent upon the quality of CUSTOMER ’s Internet connection. Inadequate Internet Connectivity is outside the scope of JUMP Technology Services’ responsibility and should be addressed by CUSTOMER directly with the Internet Service Provider. JUMP Technology Services cannot be held responsible for Internet infrastructure failures, but will aid Customer in determining the proper internet speed needed.

Service includes the following:

- Access to SSC via customer portal by up to five (5) designated CUSTOMER contacts
- Web access provides
    - Submitting Program inquiries or reporting Program problems
    - Access to Program technical tips
    - Access to Program problem and solution list(s)
    - Review CUSTOMER call/issue & status
    - Review CUSTOMER maintenance contract status

3.0 Reporting Cases to the SSC

3.1 All Program inquiries or issue reports submitted to JUMP Technology Services Help Desk Tickets (HDT) must be made by a designated CUSTOMER contact. HDT will generally fall into one of four categories:

- **Technical Assistance**: Questions about Program usage and installation that do not result in registration of a program defect or enhancement request.
- **Program Defect:** A CUSTOMER encounters a problem that is determined to be an Error or defect in the Program.
- **Feature Enhancements Requests**: Request for a tool or feature that is not included in the current set of JUMP Technology Services produced or licensed software or features. JUMP will review CUSTOMER's requests for feature enhancement during normal JUMP systems update cycles.
- **Documentation Discrepancies.**

3.2 All HDT submitted to the SSC shall be made in the form of an issue report and may require the following information prior to acknowledgment:

- Contact information for the designated CUSTOMER contact reporting the problem.
- A general description of the operating environment in which the issue was discovered (as applicable).
- A description of relevant hardware components in the environment.
- A description of relevant software components (operating system, browser) in the environment and their versions.
- A description of the problem, including screenshots, and expected results.
- System generated error messages.

3.3 JUMP will respond to HDT within JUMP's published response time goals as follows for all issues categories excluding enhancement requests:

Priority	Acknowledgment	Response
1- High	2 business hours	4 business hours
2- Medium	4 business hours	1 business day
3- Low	1 business day	3 business days

- **Acknowledgment Time** is the time between the CUSTOMER reporting the HDT to JUMP and the time JUMP gives the CUSTOMER notice that it acknowledges the situation. These response times apply to HDT reported via our ticket system during normal business hours (CST). HDT reported via the portal outside of normal business hours (CST) will adhere to the above times from the start of the next business day. Acknowledgment is dependent upon JUMP receiving sufficient information to troubleshoot the reported problem.

- **Response Time** is the time between the CUSTOMER reporting the HDT and the time that a Project Manager or SSC Analyst is assigned and actively working on the HDT.

Enhancements requests will be acknowledged within 5 business days. Response times will vary by enhancement. Enhancement credits included in annual subscription pricing shall not exceed the annual credits budgeted and shall not accrue. Requests for enhancements or services beyond the scope of this agreement shall be offered to CUSTOMER according to JUMP's current hourly support pricing.

4.0 Definitions of HDT Priorities

4.1 Priority Definitions: JUMP and CUSTOMER will work jointly to assign the appropriate priority to all HDT based on the following criteria:

Priority	Conditions
1- High	Critical business impact. The CUSTOMER has complete loss of service and work cannot reasonably continue; experiences real or perceived data loss or corruption; an essential part of the system is unusable for the CUSTOMER , which results in the inability to use a mission critical application.

2- Medium	Some business impact. The problem seriously affects the functionality of the Program but can be circumvented so that the Program can be used; or that the Program as a whole function but that a certain function is somewhat disabled, gives incorrect results or does not conform to the specifications.
3- Low	Minimal business impact. The CUSTOMER can circumvent the problem and use the system with only slight inconvenience. The error can be considered insignificant and has no significant effect on the usability of the software, e.g., a small system error or a small error in the documentation. This priority is also used for questions, comments, and requests for enhancements to the software.

4.2 JUMP's Undertaking: For each HDT reported by CUSTOMER , JUMP undertakes to:

- Maintain a telephone number for CUSTOMER to call to report a problem and receive assistance for afterhours critical outages
- Confirm receipt of all reports to CUSTOMER . The confirmation shall be in written form and shall contain an identifying ticket number assigned by JUMP which will be used in all subsequent communications and contain a timeframe in which a response from JUMP can be expected.
- Analyze the report and verify the existence of the problem
- Give CUSTOMER direction and assistance in resolving technical issues.

4.3 CUSTOMER's **Undertaking:** Before escalating a HDT to JUMP, CUSTOMER undertakes to:

- Appoint designated Contacts from CUSTOMER's organization for all matters relating to the support issues for JUMP systems
- Obtain all necessary information as outlined above.
- Include JUMP's identifying HDT number in all subsequent communications with JUMP regarding the HDT.
- Maintain an accurate record of all HDT actions, based on feedback from JUMP.

4.1 Closure of HDT

HDT will be considered to be resolved and will be closed under the following conditions:

- CUSTOMER receives an error correction, a workaround, or information that resolves the issue.
- Issue is identified as not a problem with the JUMP product
- If the HDT results in a defect correction or enhancement request being entered and CUSTOMER has been advised of this and has been notified of the defect/enhancement ID for future reference.

The HDT will be closed if the CUSTOMER has not responded after 10 business days. **Releases**

CUSTOMER may access system release information through the SSC website https://jumpssc.com

7.0 Failure Correction Goals

HDT that result in the identification of a software system defect/failure will cause a Defect to be logged. The CUSTOMER will be notified that the defect/failure was received and will be provided with an HDT number. JUMP will respond to defect reports as indicated in the table below. The response time goals do not apply in situations where it is verified that the source of the failure is a third party product.

Defect Correction Goals:

Priority	Interim Solution	Final Solution
1- High	All commercially reasonable effort until the defect is repaired	Permanent correction within 30 business days of identification of the cause of the defect
2- Medium	N/A	Permanent correction within 45 business days of identification of the cause of the defect
3- Low	N/A	Permanent correction with next schedule Major Release or Update Release

8.0 JUMP Technology Services Company Holidays

The following JUMP Technology services company holidays will be excluded from the support plan. JUMP company holidays are subject to change from year to year, but the total number of JUMP company holidays will not exceed ten (10) days per year.

Generally, the following holidays will be observed: New Year's Day, President's Day, Memorial Day, Independence Day, Labor Day, Veteran's Day, Thanksgiving Day after Thanksgiving, Christmas Day, and the Day after Christmas.

Schedule C: Training

1.0 Intellectual Property

1.1. Any ideas, concepts, know-how or data processing techniques, developed by JUMP personnel (alone or jointly with the CUSTOMER) in connection with consulting services provided under this agreement are the exclusive property of JUMP.

2. Web Based Training

2.1. All training requests will be scheduled by CUSTOMER representative through JUMP's web portal.

2.2. Cancelation and rescheduling must be coordinated by CUSTOMER representative rather than end users.

2.3. All cancelations to scheduled training must be made 48 hours prior to the scheduled training session. Cancelations less than 48 hours from the scheduled training session may result in $150 cancelation charge.

2.4. JUMP shall provide a qualified trainer for each web based training class ordered by CUSTOMER.

3. On-Site Training

3.1. CUSTOMER shall provide facilities and equipment for all onsite trainings. For initial training, CUSTOMER shall provide an appropriate training room, with a computer and high speed internet connection for each student and the JUMP trainer as well as a linked projector suitable for use with the provided trainer computer and a projection screen.

3.2. JUMP shall provide a qualified trainer for each on-site training class ordered by CUSTOMER.

3.3. JUMP shall provide a training version of the system.

3.4. All on-site training classes require four weeks' notice of cancelation. Cancelations less than four weeks prior to the training date may results in a $600 cancelation charge.

4. Training System for CUSTOMER Led Training

4.1. CUSTOMER may utilize the JUMP training or testing system to conduct CUSTOMER led training.

4.2. CUSTOMER acknowledges that the training and/or testing system is part of JUMP'S temporary staging and development environment and is not guaranteed to be available without interruption.

4.3. CUSTOMER acknowledges that the training system, when available, is offered without warranty and that CUSTOMER will not use the training system to enter electronic protected health information (ePHI).

4.4. CUSTOMER will maintain all rights and privileges to its specific database content. JUMP shall have no rights or privileges to database content, other than as required to implement JUMP technology and for the purpose of training, research, support, and maintenance of the licensed software.

Schedule D: Statement of Services

CUSTOMER is subscribing to licensing and hosting of the following system.

The data classification is:

Confidential: Personally, identifying information

Applicable governance standards for data security (Y/N):

NO - PCI: Payment card industry. The system does not store credit card and financial account information. CUSTOMER agrees not to enter this type data into the system (Warranties 10.1).

YES – HIPAA, ePHI. The system is not a healthcare system and is not offered for the purposes of providing health care, medical diagnosis, medical billing, or medical health plans. CUSTOMER agrees not to enter this type data into the system (Warranties 10.1).

Item	Description	Eff Date	End Date	Qty	Price	Extended
Home Safe Reporting Modules	Module includes: Maintenance of Home Safe Assessment, Statio portal for data correction and partner program sharing capability, download of HMIS data set, download of HSAPS19, import to HHDRS, ticket system support of product module, and training materials.	07/01/2026	06/30/2027	12	$1,829.07	$21,948.84
LEAPS Per User	License and Hosting for 300-400 users	07/01/2026	06/30/2027	1	$155,015.00	$155,015.00
Systems Modification Block Time		07/01/2026	06/30/2027	1	$17,500.00	$17,500.00
Home Safe Reporting Modules	Module includes: Maintenance of Home Safe Assessment, Statio portal for data correction and partner program sharing capability, download of HMIS data set, download of HSAPS19, import to HHDRS, ticket system support of product module, and training materials.	07/01/2027	06/30/2028	12	$1,829.07	$21,948.84
LEAPS Per User	License and Hosting for 300-400 users	07/01/2027	06/30/2028	1	$155,015.00	$155,015.00
Systems Modification Block Time		07/01/2027	06/30/2028	1	$17,500.00	$17,500.00
Home Safe Reporting Modules	Module includes: Maintenance of Home Safe Assessment, Statio portal for data correction and partner program sharing capability, download of HMIS data set, download of HSAPS19, import to HHDRS, ticket system support of product module, and training materials.	07/01/2028	06/30/2029	12	$1,829.07	$21,948.84
LEAPS Per User	License and Hosting for 300-400 users	07/01/2028	06/30/2029	1	$155,015.00	$155,015.00
Systems Modification Block Time		07/01/2028	06/30/2029	1	$17,500.00	$17,500.00
Home Safe Reporting Modules	Module includes: Maintenance of Home Safe Assessment, Statio portal for data correction and partner program sharing capability, download of HMIS data set, download of HSAPS19, import to HHDRS, ticket system support of product module, and training materials.	07/01/2029	06/30/2030	12	$1,829.07	$21,948.84
LEAPS Per User	License and Hosting for 300-400 users	07/01/2029	06/30/2030	1	$155,015.00	$155,015.00

RIVERSIDE COUNTY
DEPARTMENT OF PUBLIC SOCIAL SERVICES

Administrative Office
4060 County Circle Drive, Riverside, CA 92503
951.358.3000 FAX: 951.358.3036
www.dpss.co.riverside.ca.us

Charity Douglas, Director

Date: Wednesday, May 20, 2026

From: Charity Douglas, Director DPSS

To: Board of Supervisors

Via: Tracy Chappell Slaughter, Contracts & Grants Analyst, trchappe@rivco.org

Subject: Request for ASD Case Management System

The below information is provided in support of my department requesting review for a single or sole source purchase/agreement with a cost of $5,000 or more for goods and/or services.

☐ Single Source ☒ Sole Source

Supporting Documents: indicate which are included in the request from the list below.

☐ Supplier Quote ☒ Supplier Sole Source Letter ☒ Final draft agreement

☐ Final draft Form 11 ☐ H-11 approved by RCIT/TSOC ☐ Grant Agreement

☐ Other: _____ (i.e. CA Secretary of State Business Entity Information, Dept. of Justice Registration Conformation for non-profits, etc.)

1. Requested Supplier Name: JUMP Technology Services, L.L.C. Supplier ID: 0000120941

   a. **Describe the goods/service being requested:**
   A cloud-based case management system provided by JUMP Technology Services, L.L.C. "Jump" as a Software-as-a-Services (SaaS), including associated maintenance and support, to enhance the Adult Services Division's (ASD) ability to receive, respond to, and document reports of dependent and elder adult abuse within Riverside County.

   b. **Explain the unique features of the goods/services being requested from this supplier:**
   LEAPS supports Adult Protective Services programs in California operating under California's Welfare and Institutions Code 15640 with compliant functionality for state mandated reporting. LEAPS is proprietary software owned by JUMP

Technology Services, LLC. Licensing and distribution exclusively available from JUMP Technology Services, LLC.

JUMP can perform enhancements or modifications to the APS LEAPS system. Since the LEAPS system is deployed in 54 of California's 58 counties, the system automatically generates reports and offers cross reporting to other LEAPS counties to allow DPSS to review intakes from other counties. LEAPS users are also able to click to generate a cross report which appears in the receiving county's intake list for the counties that utilize LEAPS. The receiving county is able to view the name of the county who sent the report. This important feature saves time and increases the accuracy of the cross reported information. In addition, JUMP also provides FedRAMP certified cloud environment to provide security of PII data. JUMP provides smart mobile data captures that allow ASD to collect data while in the field.

c. **What are the operational benefits to your department?**
The LEAPS system allows ASD to receive and respond to reports of dependent adults and elder abuse in Riverside County and enter this information into the LEAPS database. The system allows ASD to have a streamlined record management system that prevents duplication and reflect accuracy when entering information. The software provides ASD with a comprehensive information management solution that promotes the health and safety of vulnerable adults. Additionally, the system allows for third-party access to the LEAPS system to support automated report/form generation, public referral submissions via web-based forms, direct referral delivery to ASD intake staff, and cross-county reporting among LEAPS agencies. LEAP pricing is based on user license levels. This simplifies procurement and budgeting allowing programs to access additional licenses with flexibility as their program grows. Also, a formal procurement for this software would be cost prohibitive given the fact that the software has been deemed compliant with WIC codes and implemented state-wide with other counties. _____

d. **Provide details on any cost benefits/discounts.**
The total cost has only increased 3% to reflect adjustments for inflation rather than substantive rise in service charges. This shows that there is modest adjustment for inflation rather than a rise in service charges. The minimal increase demonstrates JUMP's continued commitment to cost stability and long-term partnership with the County. Additionally, maintaining continuity with the existing LEAPS infrastructure avoids disruptions to critical program operations and preserves the substantial investments already made in system development, staff training, and workflow integration. When viewed in this context, the 3% increase is both justified and cost-effective for the County. When a JUMP LEAPS customer includes a new feature as part of their onboarding process, the tool becomes

available as an enhancement at no charge in the next version for all LEAPS customers.

2. **Can this request be formally bid out or procured using a viable solution such as an existing cooperative agreement or existing contract with another department or public entity?**

☐ Yes ☒ No

a. If yes, please explain why you are requesting to utilize an SSJ process? _____

3. **Has your department previously requested/received an assigned tracking number for a single or sole source request for this Supplier for the goods/service requested now?** *(If yes, please provide the reviewed single or sole source tracking number)*.

☒ Yes SSJ# *518882321 (via Rivco Pro) FY 20/21-25/26* ☐ No

a. What was the total annual and aggregate amount? $189,950 annual / $940,967 aggregate

4. **Identify all costs for this requested in the table below:**
If review is for multiple years, all costs must be identified below:
The total MRA for five (5) years is $972,325, including all expenses.

Description:	**FY 26/27**	**FY 27/28**	**FY 28/29**	**FY 29/30**	**FY 30/31**
User Subscriptions:	$155,015	$155,015	$155,015	$155,015	$155,015
Home Safe Data Support	$21,950	$21,950	$21,950	$21,950	$21,950
Enhancement Budget:	$17,500	$17,500	$17,500	$17,500	$17,500
Total Costs:	$194,465	$194,465	$194,465	$194,465	$194,465

Note: Insert additional rows as needed

* Additional compenstaion of $194,465 for a total of $1,166,790

5. **Period of Performance:** July 1, 2026 – June 30, 2031

Ratify Start Date (if applicable): _____

Initial Term Start Date: July 1, 2026 End Date: June 30, 2031

Number of renewal options (please provide those options: (i.e., one year with an option to renew four additional one-year periods): _____

Aggregate Term/End Date: June 30, 2031

6. Projected Board of Supervisor Date (if applicable): June 23, 2026

By signing below, I certify that all contractual and legal requirements to do business with the selected supplier has been fully vetted and approved.

Charity Douglas	Charity Douglas	05/26/2026
Print Name	**Department Head Signature** (Executive Level Designee)	**Date**

PCS Reviewed:

	Kimberly Cruz, Supervising PCS	06/09/2026
Print Name	**Signature**	**Date**

Note: Once signed by the Department Head and PCS (signature lines above), the PCS will e-mail completed SSJ form with supporting documents to **psolesource@rivco.org**, and cc: Supervising PCS. Please reach out to your assigned PCS with any questions.

The section below is to be completed by the Purchasing Agent or designee.

Purchasing Department Review and Comments: _____

Not to exceed:

☐ One-time $_____

☒ Annual Amounts reflected in completed chart for Question #4

Total Cost $ 1,166,790

☐ Aggregate Amount $_____

Stacy Orton	6/11/2026	26-203
Purchasing Agent Signature	**Date**	**Tracking Number** (Reference on Purchasing Documents)