CONTRACT BETWEEN THE COUNTY OF SANTA CLARA AND EXEMPLAR HUMAN SERVICES, LLC

1. This Contract is between the County of Santa Clara (henceforth, COUNTY) and Exemplar Human Services, LLC (henceforth, CONTRACTOR) for Reporting Tools and Services.

2. The parties agree to comply with the General Terms and Conditions contained in Articles I-V of this Contract and provisions contained in Exhibit A: Program Provisions, Exhibit B: Scope of Service, Exhibit C: Contractor Access Security Statement, Exhibit D: Online Privacy and Security Training, Exhibit E: CalSAWS Information Security Policy, and Exhibit F: County Information Technology User Responsibility, Exhibit G: Budget, and Exhibit H: Logic Model, which are attached hereto and incorporated herein by this reference and made a part of this Contract.

IN WITNESS WHEREOF, COUNTY and CONTRACTOR hereby agree to the terms of this Contract.

COUNTY OF SANTA CLARA

Susan Ellenberg

Susan Ellenberg
President, Board of Supervisors
Date: FEB 06 2024

CONTRACTOR

DocuSigned by:
Andrew S Bush

Andrew Bush
CEO, Exemplar Human Services LLC
Date: 1/8/2024

Signed and certified that copy of this document has been delivered by electronic or other means to the President, Board of Supervisors.

ATTEST:

Curtis Boone
Acting Clerk of the Board of Supervisors

Date: FEB 06 2024

APPROVED AS TO FORM AND LEGALITY

DocuSigned by:
Katherine Erickson

Katherine Erickson, Deputy County Counsel
Date: 1/4/2024

Approved: 02/06/2024

23-1840

FEB 06 2024

Contract General Terms and Conditions

Article I
General Terms

1. **ENTIRE CONTRACT**
This Contract and its Exhibits/Appendices (if any) constitutes the final, complete and exclusive statement of the terms of the agreement between the parties. It incorporates and supersedes all the agreements, covenants and understandings between the parties concerning the subject matter hereof, and all such agreements, covenants and understandings have been merged into this Contract. No prior or contemporaneous agreement or understanding, verbal or otherwise, of the parties or their agents shall be valid or enforceable unless embodied in this Agreement.

2. **AMENDMENTS**
This Contract may only be amended by written instrument and signed by authorized representatives of all contracting parties.

3. **CONFLICTS OF INTEREST; POLITICAL REFORM ACT**

a. CONTRACTOR shall comply, and require its subcontractors to comply, with all applicable (i) requirements governing avoidance of impermissible client conflicts; and (ii) federal, state and local conflict of interest laws and regulations including, without limitation, California Government Code section 1090 et. seq., the California Political Reform Act (California Government Code section 87100 et. seq.) and the regulations of the Fair Political Practices Commission concerning disclosure and disqualification (2 California Code of Regulations section 18700 et. seq.). Failure to do so constitutes a material breach of this Agreement and is grounds for immediate termination of this Agreement by the COUNTY.

b. In accepting this Agreement, CONTRACTOR covenants that it presently has no interest, and will not acquire any interest, direct or indirect, financial or otherwise, which would conflict in any manner or degree with the performance of this Agreement. CONTRACTOR further covenants that, in the performance of this Agreement, it will not employ any CONTRACTOR or person having such an interest. CONTRACTOR, including but not limited to CONTRACTOR's employees and subcontractors, may be subject to the disclosure and disqualification provisions of the California Political Reform Act of 1974 (the "Act"), that (1) requires such persons to disclose economic interests that may foreseeably be materially affected by the work performed under this Agreement, and (2) prohibits such persons from making or participating in making decisions that will foreseeably financially affect such interests.

c. If the disclosure provisions of the Political Reform Act are applicable to any individual providing service under this Agreement, CONTRACTOR shall, upon execution of this Agreement, provide the COUNTY with the names, description of individual duties to be performed, and email addresses of all individuals, including but not limited to CONTRACTOR's employees, agents and subcontractors, that could be substantively involved in "making a governmental decision" or "serving in a staff capacity and in that capacity participating in making governmental decisions or performing duties that would be performed by an individual in a designated position," (2 CCR 18700.3), as part of CONTRACTOR's service to the COUNTY under this Agreement. CONTRACTOR shall immediately notify the COUNTY of the names and email addresses of any additional individuals later assigned to provide such service to the COUNTY under this Agreement in such a capacity. CONTRACTOR shall immediately notify the COUNTY of the names of individuals working in such a capacity who, during the course of the Agreement, end their service to the COUNTY.

d. If applicable, CONTRACTOR and its agents shall comply with California Government Code section 84308 ("Levine Act") and the applicable regulations of the Fair Political Practices Commission concerning campaign disclosure (2 California Code of Regulations sections 18438.1 – 18438.8), which (1) require a party to a proceeding involving a contract to disclose on the record of the proceeding any contribution, as defined by Government Code section 84308(a)(6), of more than $250 that the party or their agent has made within the prior 12 months, and (2) prohibit a party to a proceeding involving a contract from making a contribution, as defined by Government Code section 84308(a)(6), of more than $250 to any COUNTY officer during the proceeding and for 12 months following the final decision in the proceeding. Disclosures pursuant to the Levine Act must be submitted online at the Office of the Clerk of the Board of Supervisors website at *http://www.sccgov.org/levineact.*

4. GOVERNING LAW, VENUE

This Contract has been executed and delivered in, and shall be construed and enforced in accordance with, the laws of the State of California. Proper venue for legal action regarding this Agreement shall be in the County of Santa Clara.

5. ASSIGNMENT

No assignment of this Contract or of the rights and obligations hereunder shall be valid without the prior written consent of the other party.

6. WAIVER

No delay or failure to require performance of any provision of this Contract shall constitute a waiver of that provision as to that or any other instance. Any waiver granted by a party shall be in writing and shall apply to the specific instance expressly stated.

7. INDEPENDENT CONTRACTOR STATUS

CONTRACTOR will perform all work and services described herein as an independent contractor and not as an officer, agent, servant, or employee of COUNTY. None of the provisions of this Contract is intended to create, nor will be deemed or construed to create, any relationship between the parties other than that of independent parties contracting with each other for purpose of effecting the provisions of this Contract. The parties are not, and will not be construed to be in a relationship of joint venture, partnership, or employer-employee. Neither party has the authority to make any statements, representations, or commitments of any kind on behalf of the other party, or to use the name of the other party in any publications or advertisements, except with the written consent of the other party or as is explicitly provided herein. CONTRACTOR is solely responsible for the acts and omissions of its officers, agents, employees, contractors, and subcontractors, if any.

8. **SEVERABILITY OF PROVISIONS**
If any provision(s) of this Contract are held invalid, the remainder of this Contract remains in force.

Article II
Fiscal Accountability and Requirements

1. **AVAILABILITY AND SUBSTITUTION OF FUNDS**
   a. Notwithstanding any provision herein, this Contract is valid and enforceable only if sufficient funds are available. In the event of reduction, suspension, discontinuance, or other unavailability of funds, COUNTY unilaterally may take appropriate actions including, but not limited to, reducing existing service authorization, immediate termination of the Contract, or reducing the maximum dollar amount of this Contract with no liability occurring to the COUNTY.

   b. The COUNTY may substitute State or Federal funds for funds appropriated by the Board of Supervisors for payments to be made pursuant to this Contract. CONTRACTOR will then be bound by the requirements of any State or Federal grant contracts, statutes, regulations, guidelines, or directives associated with the funds.

2. **COMPENSATION TO CONTRACTOR**
Compensation method shall be Fee for Service.

3. **DISALLOWED COSTS**
   a. CONTRACTOR is liable for any funds expended that are not in accordance with this Contract, including, but not limited to, disallowed costs, violation, and/or default of Contract. CONTRACTOR will repay COUNTY disallowed costs, violation and/or default amounts within ninety (90) days of discovery of these costs. This provision survives the termination of this Contract.

   b. If funding under this Contract are from Federal sources, such funds may not be used by CONTRACTOR, either directly or indirectly, as a contribution for the purpose of obtaining any Federal funds under any Federal programs. An indirect use of such funds to match Federal funds is defined as: “the allocation by CONTRACTOR of funds received under this Contract to a non-matching expenditure, thereby releasing or displacing other of its funds for the purpose of matching Federal funds.”

4. **FINANCIAL RECORDS**
   a. CONTRACTOR will establish and maintain a system of financial controls and accounting in conformance with Generally Accepted Accounting Principles (GAAP).

   b. CONTRACTOR must maintain accurate and complete financial records of all costs and operating expenses in connection with this Contract including, but not limited to subcontracts, invoices, timecards, cash receipts, vouchers, canceled checks, bank Statements, and other official documentation indicating in proper detail the nature and propriety of all costs incurred, and reimbursed by COUNTY.

c. The financial records must show that funds received under this Contract are used for purposes consistent with the terms of this Contract.

Article III
Reporting, Records, Audit, Evaluations, and Termination

1. <u>INSPECTION AND AUDIT</u>

a. All records, books, reports, and documentation maintained by CONTRACTOR pursuant to this Contract, or related to the CONTRACTOR's activities and expenditures under this Contract, will be open for inspection and audit by Federal, State, and County officials, or their agents, upon demand at reasonable times. Such records must be kept in the State of California for the retention period specified in this Contract. This provision survives the termination of this contract.

b. CONTRACTOR will provide the Federal, State, or County officials, or their agents' reasonable access, through representatives of CONTRACTOR, to facilities, records, clients, and employees that are used in conjunction with the provision of contract services, except where prohibited by Federal or State laws, regulations or rules.

c. CONTRACTOR must submit to COUNTY audited financial reports conducted by an independent certified public accountant no later than four (4) months after the end of the last month of the contract term, indicating that reported costs are actual, reasonable, necessary, allowable, and computed in accordance with GAAP and provisions stipulated in this Contract. In addition, the CONTRACTOR must submit any management letters or management advisory letters that apply to the CONTRACTOR's agency audit. COUNTY has the discretion to only require an audit report every two (2) years.

d. COUNTY may elect to accept an audit report in accordance with GAAP conducted to meet compliance requirements of other funding entities in the event all of the above provisions are met.

2. <u>REPORTING REQUIREMENTS</u>

a. CONTRACTOR must maintain complete and accurate records of its operation, including any and all records required by COUNTY relating to matters covered by this Contract, including, but not limited to, financial records, supporting documents, client statistical records, personnel and all other pertinent records. COUNTY may receive copies of any and all such records upon request.

b. CONTRACTOR must submit to COUNTY a compensation claim on forms approved by COUNTY Social Services Agency.

c. CONTRACTOR must assist COUNTY in meeting COUNTY's reporting requirements to the State and other agencies with respect to CONTRACTOR's work hereunder. This cooperation includes assisting COUNTY to prepare evaluations required by the State or Federal governments regarding services provided by CONTRACTOR under this Contract. CONTRACTOR must submit to COUNTY any and all reports that may be required by COUNTY concerning CONTRACTOR's performance under this Contract.

d. Upon COUNTY's request, CONTRACTOR must provide COUNTY evidence of CONTRACTOR's capacity to perform under this Contract, its compliance with applicable statutes and regulations, and its compliance with the terms and conditions of this Contract.

e. All records, books, reports and documentation must be retained in the State of California by CONTRACTOR for four (4) years after termination of this Contract; or until all Federal, State and County audits are completed; or until all disputes, litigation, or claims are resolved; whichever is later. All such records, books, reports and documentation must be transmitted to the COUNTY of Santa Clara, Social Services Agency in the event that CONTRACTOR goes out of business during the period in which records are required to be maintained. This provision survives the termination of this contract.

f. CONTRACTOR must within 30 calendar days advise the COUNTY of 1) the issuance of any legal complaint by an enforcement agency, or any enforcement proceedings by any Federal, State or local agency for alleged violations of Federal, State or local rules, regulations or laws, and/or 2) the issuance of citations, court findings or administrative findings for violations of applicable Federal, State or local rules, regulations or laws.

g. CONTRACTOR guarantees that it, its employees, contractors, subcontractors or agents are not suspended or debarred from receiving Federal fund as listed in the List of Parties Excluded from Federal Procurement or Non-procurement Programs issued by the Federal General Services Administration (https://www.sam.gov/). CONTRACTOR must within 30 calendar days advise the COUNTY if it, its employees, contractors, subcontractors or agents become suspended or debarred from receiving Federal funds as listed in the List of Parties Excluded from Federal Procurement or Non-procurement Programs issued by the Federal General Services Administration during the term of this Agreement.

3. RESPONSIBILITY FOR AUDIT EXCEPTIONS

CONTRACTOR accepts responsibility for receiving, replying to, and complying with any audit exceptions by appropriate Federal, State, or County, audit agencies.

4. MONITORING AND EVALUATION

a. COUNTY's Social Services Agency will monitor the work performed and financial operations conducted under this Contract to determine whether CONTRACTOR's operation conforms to County policy, Federal and State statutes and regulations, and to the terms of this Contract.

b. COUNTY may conduct participant interviews to determine program compliance.

c. CONTRACTOR agrees to participate in and cooperate with studies and surveys

COUNTY deems necessary to meet its monitoring and evaluation responsibility.

d. CONTRACTOR must furnish all data, Statements, records, information, and reports necessary for COUNTY to monitor, review, and evaluate the performance of the program and its components. Performance evaluations will examine the following five factors: 1) fiscal accountability; 2) completion of work within a given time frame; 3) ability and effort to meet the performance criteria; 4) quality of services; and 5) a recommendation for future contracting with the CONTRACTOR.

e. If, in the course of monitoring and evaluation, COUNTY discovers any practice, procedure or policy of CONTRACTOR that deviates from the terms of this Contract; that violates State or Federal statutes or regulations; that threatens the success of the program carried on pursuant to this Contract, or that jeopardizes the fiscal integrity of said program, COUNTY may impose reasonable funding restrictions upon notice specifying the nature of the restrictions(s), reasons for imposition, the corrective action that must be taken before they will be removed, time allowed for completing the corrective action, and method of requesting reconsideration.

f. CONTRACTOR must respond in writing to any discrepancies, violations, or deficiencies identified by COUNTY within ten (10) days.

5. CORRECTIVE ACTION PROCEDURE

a. Upon receipt by COUNTY of information regarding a failure by CONTRACTOR to comply with any provision of this Contract, COUNTY has the right to forward to CONTRACTOR a notice of COUNTY’s intent to consider corrective action to enforce compliance with such provision. Such notice will indicate the nature of the issue, or issues, to be reviewed in determining the need for corrective action. CONTRACTOR may have the opportunity to respond or participate in formulating the corrective action recommendation. COUNTY has the right to require the presence of CONTRACTOR’s officer(s) or employee(s) at any hearing or meeting called for the purpose of considering corrective action.

b. After issuing such notice, and after considering CONTRACTOR’s response, if any, COUNTY may forward to CONTRACTOR a set of specific corrective actions recommended and a timetable for implementing the specified corrective actions recommended. Following implementation of the corrective actions, CONTRACTOR will forward to COUNTY, within the time specified by COUNTY, any verification required by COUNTY regarding the corrective actions.

b. In the event CONTRACTOR does not implement the corrective actions recommended in accordance with the corrective actions timetable, COUNTY may suspend payments hereunder or immediately terminate this Contract without further notice to CONTRACTOR.

6. TERMINATION

a. Termination for Convenience

COUNTY may, by written notice to CONTRACTOR, terminate all or part of this

Agreement at any time for the convenience of the COUNTY. The notice shall specify the effective date and the scope of the termination.

b. Termination for Cause
COUNTY may, at any time, elect to suspend or terminate this Contract or withhold payments to CONTRACTOR, in whole or in part, for cause, by giving written notice specifying the effective date and scope of such termination. Cause includes, but is not limited to the following:

i. CONTRACTOR failure to comply with any contract provision;
ii. CONTRACTOR fails to meet the performance criteria of this Contract;
iii. COUNTY deems CONTRACTOR's performance unsatisfactory.
iv. Litigation is pending with respect to the CONTRACTOR's performance under this Contract that may jeopardize or adversely affect services;
v. CONTRACTOR is the subject of a voluntary or involuntary proceeding under the Bankruptcy Act;
vi. CONTRACTOR submits to COUNTY any reports that are incorrect or incomplete in any material respect, or fails to file timely reports; or,
vii. CONTRACTOR is suspended or debarred from receiving Federal funds as listed in the List of Parties Excluded from Federal Procurement or Non-procurement Programs issued by the General Services Administration.

c. Terminations
In the event of any termination, all finished or unfinished documents, data, studies, reports, and materials (Materials) prepared by the CONTRACTOR under this Contract becomes the property of the COUNTY and will be promptly delivered to the COUNTY. Upon termination, the CONTRACTOR may make and retain a copy of such Materials. CONTRACTOR may be compensated based on the completion of services provided, as solely and reasonably determined by COUNTY.

7. **NON-EXCLUSIVE REMEDIES**
The remedies listed in this Contract are non-exclusive, and COUNTY retains all other rights and remedies it may have under general law, including the right to terminate the Contract immediately without advance notice if CONTRACTOR becomes unable to perform its obligations under this Contract.

Article IV
Statutes, Regulations, and Policies

1. **COMPLIANCE WITH ALL LAWS, INCLUDING NONDISCRMINATION, EQUAL OPPORTUNITY, AND WAGE THEFT PREVENTION**

a. Compliance with All Laws. CONTRACTOR shall comply with all applicable Federal, State, and local laws, regulations, rules, and policies (collectively, "Laws"), including but not limited to the non-discrimination, equal opportunity, and wage and hour Laws referenced in the paragraphs below.

b. Compliance with Non-Discrimination and Equal Opportunity Laws: CONTRACTOR shall comply with all applicable Laws concerning nondiscrimination and equal opportunity in employment and contracting, including but not limited to the following: Santa Clara County's policies for contractors on nondiscrimination and equal opportunity; Title VII of the Civil Rights Act of 1964 as amended; Americans with Disabilities Act of 1990; the Age Discrimination in Employment Act of 1967; the Rehabilitation Act of 1973 (Sections 503 and 504); the Equal Pay Act of 1963; California Fair Employment and Housing Act (Government Code sections 12900 et seq.); California Labor Code sections 1101, 1102, and 1197.5; and the Genetic Information Nondiscrimination Act of 2008. In addition to the foregoing, CONTRACTOR shall not discriminate against any subcontractor, employee, or applicant for employment because of age, race, color, national origin, ancestry, religion, sex, gender identity, gender expression, sexual orientation, mental disability, physical disability, medical condition, political belief, organizational affiliation, or marital status in the recruitment, selection for training (including but not limited to apprenticeship), hiring, employment, assignment, promotion, layoff, rates of pay or other forms of compensation. Nor shall CONTRACTOR discriminate in the provision of services provided under this contract because of age, race, color, national origin, ancestry, religion, sex, gender identity, gender expression, sexual orientation, mental disability, physical disability, medical condition, political beliefs, organizational affiliations, or marital status.

c. Compliance with Wage and Hour Laws: CONTRACTOR shall comply with all applicable wage and hour Laws, which may include but are not limited to, the Federal Fair Labor Standards Act, the California Labor Code, and, if applicable, any local Minimum Wage, Prevailing Wage, or Living Wage laws.

d. Definitions: For purposes of this Section, the following definitions shall apply. A "Final Judgment" shall mean a judgment, decision, determination, or order (a) which is issued by a court of law, an investigatory government agency authorized by law to enforce an applicable Law, an arbiter, or arbitration panel and (b) for which all appeals have been exhausted or the time period to appeal has expired. For pay equity Laws, relevant investigatory government agencies include the federal Equal Employment Opportunity Commission, the California Division of Labor Standards Enforcement, and the California Department of Fair Employment and Housing. Violation of a pay equity Law shall mean unlawful discrimination in compensation on the basis of an individual's sex, gender, gender identity, gender expression, sexual orientation, race, color, ethnicity, or national origin under Title VII of the Civil Rights Act of 1964 as amended, the Equal Pay Act of 1963, California Fair Employment and Housing Act, or California Labor Code section 1197.5, as applicable. For wage and hour Laws, relevant investigatory government agencies include the federal Department of Labor, the California Division of Labor Standards Enforcement, and the City of San Jose's Office of Equality Assurance.

e. Prior Judgments, Decisions or Orders against CONTRACTOR : BY SIGNING THIS AGREEMENT, CONTRACTOR AFFIRMS THAT IT HAS DISCLOSED ANY FINAL JUDGMENTS THAT (A) WERE ISSUED IN THE FIVE YEARS PRIOR TO EXECUTING THIS AGREEMENT BY A COURT, ANINVESTIGATORY GOVERNMENT AGENCY, ARBITER, OR ARBITRATION PANEL AND (B) FOUND THAT CONTRACTOR VIOLATED AN APPLICABLE WAGE AND

HOUR LAW OR PAY EQUITY LAW. CONTRACTOR FURTHER AFFIRMS THAT IT HAS SATISFIED AND COMPLIED WITH—OR HAS REACHED AGREEMENT WITH THE COUNTY REGARDING THE MANNER IN WHICH IT WILL SATISFY—ANY SUCH FINAL JUDGMENTS, DECISIONS, DETERMINATIONS, OR ORDERS.

f. Violations of Wage and Hour Laws or Pay Equity Laws During Term of Contract: If at any time during the term of this Agreement, CONTRACTOR receives a Final Judgment rendered against it for violation of an applicable wage and hour Law or pay equity Law, then CONTRACTOR shall promptly satisfy and comply with any such Final Judgment. CONTRACTOR shall inform the Office of the County Executive-Office of Countywide Contracting Management (OCCM) of any relevant Final Judgment against it within 30 days of the Final Judgment becoming final or of learning of the Final Judgment, whichever is later. CONTRACTOR shall also provide any documentary evidence of compliance with the Final Judgment within 5 days of satisfying the Final Judgment. Any notice required by this paragraph shall be addressed to the Office of the County Executive-OCCM at 70 W. Hedding Street, East Wing, 11th Floor, San José, CA 95110. Notice provisions in this paragraph are separate from any other notice provisions in this Agreement and, accordingly, only notice provided to the Office of the County Executive-OCCM satisfies the notice requirements in this paragraph.

g. Access to Records Concerning Compliance with Pay Equity Laws: In addition to and notwithstanding any other provision of this Agreement concerning access to CONTRACTOR's records, CONTRACTOR shall permit the COUNTY and/or its authorized representatives to audit and review records related to compliance with applicable pay equity Laws. Upon the COUNTY's request, CONTRACTOR shall provide the COUNTY with access to any and all facilities and records, including but not limited to financial and employee records, that are related to the purpose of this Section, except where prohibited by federal or state laws, regulations or rules. COUNTY's access to such records and facilities shall be permitted at any time during CONTRACTOR's normal business hours upon no less than 10 business days' advance notice.

h. Pay Equity Notification: CONTRACTOR shall (1) at least once in the first year of this Agreement and annually thereafter, provide each of its employees working in California and each person applying to CONTRACTOR for a job in California (collectively, "Employees and Job Applicants") with an electronic or paper copy of any applicable pay equity Laws, or (2) throughout the term of this Agreement, continuously post an electronic copy of all applicable pay equity Laws in conspicuous places accessible to all of CONTRACTOR's Employees and Job Applicants.

i. Material Breach: Failure to comply with any part of this Section shall constitute a material breach of this Agreement. In the event of such a breach, the County may, in its discretion, exercise any or all remedies available under this Agreement and at law. COUNTY may, among other things, take any or all of the following actions:

i. Suspend or terminate any or all parts of this Agreement.
ii. Withhold payment to CONTRACTOR until full satisfaction of a Final Judgment concerning violation of an applicable wage and hour Law or pay equity Law.
iii. Offer CONTRACTOR an opportunity to cure the breach.

j. Subcontractors: CONTRACTOR shall impose all of the requirements set forth in this Section on any subcontractors permitted to perform work under this Agreement. This includes ensuring that any subcontractor receiving a Final Judgment for violation of an applicable Law promptly satisfies and complies with such Final Judgment.

k. CONTRACTOR recognizes the mandatory standards and policies relating to energy efficiency in the State energy conservation plan (Title 24, California Administrative Code).

l. For Contracts over $100,000 CONTRACTOR will comply with all applicable standards, orders, or requirements issued under Section 306 of the Clean Air Act (42 U.S. Code 1857 (h)), Section 508 of the Clean Water Act (33 U.S. Code 1368), Executive Order 11738, and Environmental Protection Agency regulations (40 CFR Part 15).

m. CONTRACTOR must establish procedures assuring that any person's complaints and grievances against CONTRACTOR regarding the delivery of services under this Contract are promptly addressed and fairly resolved.

2. ASSIGNMENT OF CLAYTON ACT, CARTWRIGHT ACT CLAIMS

CONTRACTOR hereby assigns to the COUNTY all rights, title, and interest in and to all causes of action it may have under Section 4 of the Clayton Act (15 U.S.C. Sec. 15) or under the Cartwright Act (Chapter 2 (commencing with Section 16700) of Part 2 of Division 7 of the Business and Professions Code), arising from purchases of goods, materials, or services by the CONTRACTOR for sale to the COUNTY pursuant to this Contract.

3. COUNTY NO-SMOKING POLICY

CONTRACTOR and its employees, agents and subcontractors, shall comply with the COUNTY's No-Smoking Policy, as set forth in the Board of Supervisors Policy Manual section 3.47 (as amended from time to time), which prohibits smoking: (1) at the Santa Clara Valley Medical Center Campus and all COUNTY-owned and operated health facilities, (2) within 30 feet surrounding COUNTY-owned buildings and leased buildings where the COUNTY is the sole occupant, and (3) in all COUNTY vehicles.

4. FOOD AND BEVERAGE STANDARDS

a. Except in the event of an emergency or medical necessity, the following nutritional standards shall apply to any foods and/or beverages purchased by CONTRACTOR with COUNTY funds for COUNTY-sponsored meetings or events.

b. If food is to be provided, healthier food options must be offered. "Healthier food options" include (1) fruits, vegetables, whole grains, and low fat and low-calorie foods; (2) minimally processed foods without added sugar and with low sodium; (3) foods prepared using healthy cooking techniques; and (4) foods with less than 0.5 grams of trans fat per serving. Whenever possible, CONTRACTOR shall (1) offer seasonal and local produce; (2) serve fruit instead of sugary, high calorie desserts; (3) attempt to accommodate special, dietary and cultural needs; and (4) post nutritional information and/or a list of ingredients for items served. If meals are to be provided, a vegetarian option shall be provided, and the CONTRACTOR should consider providing a vegan option. If pre-packaged snack foods are provided, the items shall contain: (1) no more than 35% of calories from fat, unless the snack food items consist solely of nuts or seeds; (2) no more than 10% of calories from saturated fat; (3) zero trans-fat; (4) no more than 35% of total weight from sugar and caloric sweeteners, except for fruits and vegetables with no added sweeteners or fats; and (5) no more than 360 mg of sodium per serving.

c. If beverages are to be provided, beverages that meet the COUNTY’s nutritional criteria are (1) water with no caloric sweeteners; (2) unsweetened coffee or tea, provided that sugar and sugar substitutes may be provided as condiments; (3) unsweetened, unflavored, reduced fat (either nonfat or 1% low fat) dairy milk; (4) plant-derived milk (e.g., soy milk, rice milk, and almond milk) with no more than 130 calories per 8 ounce serving; (5) 100% fruit or vegetable juice (limited to a maximum of 8 ounces per container); and (6) other low-calorie beverages (including tea and/or diet soda) that do not exceed 40 calories per 8 ounce serving. Sugar-sweetened beverages shall not be provided.

5. CONTRACTING PRINCIPLES

CONTRACTOR agrees to comply with the COUNTY’s Contracting Principles set forth in the Board Policy Manual. The Contracting Principles require, among other things, that CONTRACTOR be a fiscally responsible entity and treat its employees fairly. CONTRACTOR is also required to (1) comply with all applicable federal, state and local rules, regulations and laws; (2) maintain financial records, and make those records available upon request; (3) provide to the COUNTY copies of any financial audits that have been completed during the term of the contract; and (4) upon the COUNTY's request, provide the COUNTY reasonable access, through representatives of the CONTRACTOR, to facilities, financial and employee records that are related to the purpose of the contract, except where prohibited by federal or state laws, regulations or rules. Refer to:
https://boardclerk.sccgov.org/sites/g/files/exjcpb656/files/BOSPolicyCHAP5.pdf

6. THIRD PARTY BENEFICIARIES

This agreement does not, and is not intended to, confer any rights or remedies upon any person or entity other than the parties.

7. MAINTENANCE OF SOFTWARE

If CONTRACTOR is provided with “remote access”, defined as the act of connecting to a COUNTY attached information technology system from a non-county attached system through a public network, CONTRACTOR will maintain and use its non-county system, hardware, and software in compliance with COUNTY standards and policies set by the COUNTY Information Services Department.

8. CONTRACT EXECUTION

Unless otherwise prohibited by law or County policy, the parties agree that an electronic copy of a signed contract, or an electronically signed contract, has the same force and legal effect as a contract executed with an original ink signature. The term “ELECTRONIC COPY OF A SIGNED CONTRACT” refers to a transmission by facsimile, electronic mail, or other electronic means of a copy of an original signed contract in a portable document format. The term “ELECTRONICALLY SIGNED CONTRACT” means a contract that is executed by applying an electronic signature using technology approved by the COUNTY.

9. LIVING WAGE (If Applicable)

Unless otherwise exempted or prohibited by law or County policy, where applicable, CONTRACTORs that contract with the COUNTY to provide Direct Services developed pursuant to a formal Request for Proposals process, as defined in County of Santa Clara Ordinance Code Division B36 (“Division B36”) and Board Policy section 5.5.5.5 (“Living Wage Policy”), and their subcontractors, where the contract value is $100,000 or more (“Direct Services Contract”), must comply with Division B36 and the Living Wage Policy and compensate their employees in accordance with Division B36 and the Living Wage Policy. Compliance and compensation for purposes of this provision includes, but is not limited to, components relating to fair compensation, earned sick leave, paid jury duty, fair workweek, worker retention, fair chance hiring, targeted hiring, local hiring, protection from retaliation, and labor peace. If CONTRACTOR and/or a subcontractor violate this provision, the Boar d of Supervisors or its designee may, at its sole discretion, take responsive actions including, but not limited to, the following:

a. Suspend, modify, or terminate the Direct Services Contract.

b. Require the CONTRACTOR and/or Subcontractor to comply with an appropriate remediation plan developed by the COUNTY.

c. Waive all or part of Division B36 or the Living Wage Policy.

This provision shall not be construed to limit an employee's rights to bring any legal action for violation of the employee's rights under Division B36 or any other applicable law. Further, this provision does not confer any rights upon any person or entity other than the Board of Supervisors or its designee to bring any action seeking the cancellation or suspension of a COUNTY contract. By entering into this contract, CONTRACTOR certifies that it is currently complying with Division B36 and the Living Wage Policy with respect to applicable contracts, and warrants that it will continue to comply with Division B36 and the Living Wage Policy with respect to applicable contracts.

10. COUNTY DATA & CONFIDENTIALITY

a. Definitions: “COUNTY Data” shall mean data and information received by CONTRACTOR from COUNTY. County Data includes any information or data that is transported across a County network, or that resides in a County-owned information system, or on a network or system under the control and management of a CONTRACTOR for use by COUNTY. “County Confidential Information” shall include all material, non-public information (including material, non-public County Data) appearing in any form (including, without limitation, written, oral or displayed), that is disclosed, directly or indirectly, through any means of communication by COUNTY, its agents or employees, to CONTRACTOR, its agents or employees, or any of its affiliates or representatives.

b. CONTRACTOR shall not acquire any ownership interest in County Data (including County Confidential Information). As between CONTRACTOR and COUNTY, all County Confidential Information and/or County Data shall remain the property of the COUNTY. CONTRACTOR shall not, without COUNTY's written permission, use or disclose County Data (including County Confidential Information) other than in the performance of its obligations under this Agreement.

c. CONTRACTOR shall be responsible for establishing and maintaining an information security program that is designed to ensure the security and confidentiality of County Data, protect against any anticipated threats or hazards to the security or integrity of County Data, and protect against unauthorized access to or use of County Data that could result in substantial harm or inconvenience to COUNTY or any end users. Upon termination or expiration of this Agreement, CONTRACTOR shall seek and follow COUNTY's direction regarding the proper disposition of County Data.

d. CONTRACTOR shall take appropriate action to address any incident of unauthorized access to County Data, including addressing and/or remedying the issue that resulted in such unauthorized access, and notifying COUNTY by phone or in writing within 24 hours of any incident of unauthorized access to County Data, or any other breach in CONTRACTOR's security that materially affects COUNTY or end users. If the initial notification is by phone, CONTRACTOR shall provide a written notice within 5 days of the incident. CONTRACTOR shall be responsible for ensuring compliance by its officers, employees, agents, and subcontractors with the confidentiality, privacy, and information security requirements of this Agreement. Should County Confidential Information and/or legally protected County Data be divulged to unauthorized third parties, CONTRACTOR shall comply with all applicable federal and state laws and regulations, including but not limited to California Civil Code sections 1798.29 and 1798.82 at CONTRACTOR's sole expense. CONTRACTOR shall not charge COUNTY for any expenses associated with CONTRACTOR's compliance with these obligations.

e. CONTRACTOR shall defend, indemnify and hold COUNTY harmless against any claim, liability, loss, injury or damage arising out of, or in connection with, the unauthorized use, access, and/or disclosure of information by CONTRACTOR and/or its agents, employees or sub-contractors, excepting only loss, injury or damage caused by the sole negligence or willful misconduct of personnel employed by the COUNTY.

f. CONTRACTOR must require its employees and all persons performing services at its direction to comply with all applicable privacy laws and regulations, including but not limited to the provisions of Sections 827 and 10850 et seq. of the Welfare and Institutions Code (WIC) and California Department of Social Services (CDSS) Manual of Policies and Procedures, Division 19 Regulations. Data-sharing is limited to purposes authorized under these regulations for one year only. This timeframe may be extended to June 30, 2025, without a contract amendment, following approval from Social Services Agency's System and Data Access Review Committee.

i. All applications and records concerning any individual receiving services pursuant to this contract are confidential and are not open to examination for any purpose not directly connected with the administration, performance compliance, monitoring or auditing of the program.

ii. No person may publish, disclose, use, or permit or cause to be published or disclosed; any confidential information pertaining to services, except as is provided by law.

g. Upon the disclosure of confidential information, inadvertent or otherwise, the COUNTY may terminate this contract immediately and take legal action against CONTRACTOR. Any person who knowingly and intentionally violates the provisions stated above is guilty of a misdemeanor and the COUNTY intends to prosecute such violators to the full extent of the law.

h. CONTRACTOR will inform all employees, agents, officers, and all persons performing services at its direction of the above provisions. All provisions of Article IV, Section 10. survive the termination of this contract.

11. <u>CALIFORNIA PUBLIC RECORDS ACT</u>

a. The COUNTY is a public agency subject to the disclosure requirements of the California Public Records Act ("CPRA"). If CONTRACTOR's proprietary information is contained in documents or information submitted to COUNTY, and CONTRACTOR claims that such information falls within one or more CPRA exemptions, CONTRACTOR must clearly mark such information "CONFIDENTIAL AND PROPRIETARY," and identify the specific lines containing the information. In the event of a request for such information, the COUNTY will make best efforts to provide notice to CONTRACTOR prior to such disclosure. If CONTRACTOR contends that any documents are exempt from the CPRA and wishes to prevent disclosure, it is required to obtain a protective order, injunctive relief or other appropriate remedy from a court of law in Santa Clara COUNTY before the COUNTY is required to respond to the CPRA request. If CONTRACTOR fails to obtain such remedy within the time the COUNTY is required to respond to the CPRA request, COUNTY may disclose the requested information.

b. CONTRACTOR further agrees that it shall defend, indemnify and hold COUNTY harmless against any claim, action or litigation (including but not limited to all judgments, costs, fees, and attorney's fees) that may result from denial by COUNTY of a CPRA request for information arising from any representation, or any action (or inaction), by the CONTRACTOR.

12. COVID-19 REQUIREMENTS

Contractor shall comply with all County requirements in effect relating to COVID-19 for persons who routinely perform services for County onsite and share airspace with or proximity to other people at a County facility as part of their services for County as set forth in a County Health Order (or similar directives) available at https://covid19.sccgov.org/home, and incorporated herein by this reference. Contractor shall comply with all reasonable requests by County for documentation demonstrating Contractor's compliance with this Section.

13. SURVIVAL

All representations, warranties, and covenants contained in this Contract, or in any instrument, certificate, exhibit, or other writing intended by the parties to survive this Contract, shall survive the termination or expiration of this Contract, including but not limited to all terms (1) providing for indemnification of COUNTY; (2) relating to the California Public Records Act; (3) relating to COUNTY Data; and (4) relating to CONTRACTOR's obligations upon termination or expiration of this Contract.

Article V
Insurance Requirements

INSURANCE REQUIREMENTS FOR STANDARD CONTRACTS ABOVE $100,000

Indemnity

Notwithstanding any other provision of this Agreement, Contractor shall indemnify, release, hold harmless, and defend, with counsel approved by County of Santa Clara (hereinafter "County"), County and its officers, agents, and employees from any claim, demand, suit, judgment, liability, loss, injury, damage, or expense of any kind (including attorneys' fees and costs) arising out of, or in connection with, performance of this Agreement by Contractor and/or its officers, agents, employees, or sub-contractors, excepting only loss, injury, or damage caused by the sole negligence or willful misconduct of personnel employed by County. It is the intent of the parties to this Agreement to provide the broadest possible coverage for County as allowed by law. Contractor shall reimburse County for all costs, attorneys' fees, expenses, and liabilities incurred with respect to any litigation or process in which Contractor contests its obligation to indemnify, defend, and/or hold harmless County under this Agreement and does not prevail in that contest.

Insurance

Without limiting the Contractor's indemnification of the County, the Contractor shall provide and maintain at its own expense, during the term of this Agreement, or as may be further required herein, the following insurance coverages and provisions:

A. Evidence of Coverage

Prior to commencement of this Agreement, the Contractor shall provide a Certificate of Insurance certifying that coverage as required herein has been obtained. Individual endorsements executed by the insurance carrier shall accompany the certificate. In addition, a certified copy of the policy or policies shall be provided by the Contractor upon request.

This verification of coverage shall be sent to the requesting County department, unless otherwise directed. The Contractor shall not receive a Notice to Proceed with the work under the Agreement until it has obtained all insurance required and such insurance has been approved by the County. This approval of insurance shall neither relieve nor decrease the liability of the Contractor.

B. Qualifying Insurers
All coverages, except surety, shall be issued by companies which hold a current policy holder's alphabetic and financial size category rating of not less than A- V, according to the current Best's Key Rating Guide or a company of equal financial stability that is approved by the County's Insurance Manager.

C. Notice of Cancellation
All coverage as required herein shall not be canceled or changed so as to no longer meet the specified County insurance requirements without 30 days' prior written notice of such cancellation or change being delivered to the County of Santa Clara or their designated agent.

D. Insurance Required

1. Commercial General Liability Insurance - for bodily injury (including death) and property damage which provides limits as follows:

a.	Each occurrence	-	$1,000,000
b.	General aggregate	-	$2,000,000
c.	Products/Completed Operations aggregate	-	$2,000,000
d.	Personal Injury	-	$1,000,000

2. General liability coverage shall include:

   a. Premises and Operations
   b. Products/Completed
   c. Personal Injury liability
   d. Severability of interest

3. General liability coverage shall include the following endorsement, a copy of which shall be provided to the County:

   Additional Insured Endorsement, which shall read:

   > “County of Santa Clara, and members of the Board of Supervisors of the County of Santa Clara, and the officers, agents, and employees of the County of Santa Clara, individually and collectively, as additional insureds.”

   Insurance afforded by the additional insured endorsement shall apply as primary insurance, and other insurance maintained by the County of Santa Clara, its officers, agents, and employees shall be excess only and not contributing with insurance provided under this policy. Public Entities may also be added to the additional insured endorsement as applicable and the contractor shall be notified by the contracting department of these requirements.

4. Automobile Liability Insurance
   For bodily injury (including death) and property damage which provides total limits of not less than one million dollars ($1,000,000) combined single limit per occurrence applicable to all owned, non-owned and hired vehicles.

4a. Aircraft/Watercraft Liability Insurance (Required if Contractor or any of its agents or subcontractors will operate aircraft or watercraft in the scope of the Agreement)
   For bodily injury (including death) and property damage which provides total limits of not less than one million dollars ($1,000,000) combined single limit per occurrence applicable to all owned, non-owned and hired aircraft/watercraft.

5. Workers' Compensation and Employer's Liability Insurance
   a. Statutory California Workers' Compensation coverage including broad form all-states coverage.
   b. Employer's Liability coverage for not less than one million dollars ($1,000,000) per occurrence.

6. Cyber Liability

a.	Each occurrence	-	$1,000,000
b.	General aggregate	-	$2,000,000

7. Cyber liability coverage shall include at a minimum, but not limited to:
   a. Information Security and Privacy Liability
   b. Privacy Notification Costs

E. Special Provisions
The following provisions shall apply to this Agreement:

1. The foregoing requirements as to the types and limits of insurance coverage to be maintained by the Contractor and any approval of said insurance by the County or its insurance consultant(s) are not intended to and shall not in any manner limit or qualify the liabilities and obligations otherwise assumed by the Contractor pursuant to this Agreement, including but not limited to the provisions concerning indemnification.

2. The County acknowledges that some insurance requirements contained in this Agreement may be fulfilled by self-insurance on the part of the Contractor. However, this shall not in any way limit liabilities assumed by the Contractor under this Agreement. Any self-insurance shall be approved in writing by the County upon satisfactory evidence of financial capacity. Contractors obligation hereunder may be satisfied in whole or in part by adequately funded self-insurance programs or self-insurance retentions.

3. Should any of the work under this Agreement be sublet, the Contractor shall require each of its subcontractors of any tier to carry the aforementioned

coverages, or Contractor may insure subcontractors under its own policies.

4. The County reserves the right to withhold payments to the Contractor in the event of material noncompliance with the insurance requirements outlined above.

F. Fidelity Bonds (Required only if contractor will be receiving advanced funds or payments)
Before receiving compensation under this Agreement, Contractor will furnish County with evidence that all officials, employees, and agents handling or having access to funds received or disbursed under this Agreement, or authorized to sign or countersign checks, are covered by a BLANKET FIDELITY BOND in an amount of AT LEAST fifteen percent (15%) of the maximum financial obligation of the County cited herein. If such bond is canceled or reduced, Contractor will notify County immediately, and County may withhold further payment to Contractor until proper coverage has been obtained. Failure to give such notice may be cause for termination of this Agreement, at the option of County.

Exhibit A: Program Provisions

CONTRACTOR: Exemplar Human Services, LLC

PROGRAM/PROJECT NAME: Reporting Tools and Services

1. SCOPE OF SERVICE

CONTRACTOR staff who are approved by COUNTY shall receive access to the CalSAWS system for purposes directly connected with providing a portfolio of reporting tools to assist Department of Employment and Benefits Services (DEBS) staff with their workload and meeting service and performance outcomes. CONTRACTOR staff who are approved by COUNTY shall receive access to the California Statewide Automated Welfare System (CalSAWS) to help develop reports that will optimize DEBS daily operations.

2. DELIVERABLES

a. CONTRACTOR will provide, at minimum, the following types of reports:

   i. Intake Productivity Report
   ii. Continuing Productivity Report
   iii. Welfare to Work Productivity Report
   iv. Productivity/Tele-work Report
   v. Intake Pending Apps Report
   vi. Continuing Eligibility Report
   vii. Welfare to Work Alerts Report
   viii. Executive Dashboard (Monthly) Report
   ix. Power Business Intelligence (PBI) Suite of Report
   x. All reporting tools to be provided daily and to all DEBS staff unless otherwise directed by executive staff.

b. Invoices

CONTRACTOR will submit invoices in a format approved by COUNTY and as outlined in Section 6 of this Exhibit. Invoices must be signed by CONTRACTOR.

c. SSA Outcome Measurement Reporting

CONTRACTOR will submit a quarterly report as outlined in Section 7 of this Exhibit and Exhibit H: Logic Model

3. TERM OF CONTRACT

The term begins upon execution, and expires on June 30, 2025, unless terminated earlier or otherwise amended.

4. MAXIMUM FINANCIAL OBLIGATION

COUNTY will reimburse CONTRACTOR actual allowable expenditures subject to the provisions of this Contract, for a total not to exceed $175,000 for Fiscal Year (FY) 2024, $420,000 for FY2025 for a total of $595,000.

5. BUDGET CONTINGENCY

This Contract is contingent upon the appropriation of sufficient funding by COUNTY for the services covered by this Contract. Notwithstanding the termination provisions set forth herein, if funding is reduced or depleted by COUNTY for services covered by this Contract, COUNTY has the option to either terminate this Contract without notice (except that necessary to transition clients in the discretion of COUNTY) and with no liability occurring to COUNTY, or to offer an amendment to this Contract indicating the reduced amount.

6. COMPENSATION TO CONTRACTOR

a. FEE FOR SERVICE CONTRACT

i. CONTRACTOR will be paid by COUNTY in accordance with Exhibit A: Program Provisions, Exhibit B: Scope of Work, and Exhibit G: Budget, for the performance of services as outlined in this Contract up to the maximum compensation. These costs will also be in accordance with current cost principles and with all other requirements of this contract:

1. For Non-Profit Agencies, OMB Circular A-122.
2. For Local Governments, OMB Circular A-87.
3. For Public and Nonprofit Institutions of Higher Education, OMB Circular A-121.
4. For Profit Making Organization, 41 CFR Part 1.

ii. If CONTRACTOR provides any tasks, deliverables, goods, services, or other work, other than as specified in this Contract, the same will be deemed to be a gratuitous effort on the part of CONTRACTOR, and CONTRACTOR will have no claim whatsoever against COUNTY.

iii. CONTRACTOR must participate in a closeout period at the end of the COUNTY funding period. During the closeout period all funds awarded to CONTRACTOR must be reconciled to the costs incurred and to the remaining cash, if any. A closeout packet will be provided to CONTRACTOR by COUNTY at the end of the funding period and is due within forty-five (45) days thereafter. This provision survives the termination of this Contract.

b. COMPENSATION

CONTRACTOR must submit to COUNTY an invoice in a form approved by COUNTY, by the tenth (10th) working day of each month for the month just preceding in which services were performed. The CONTRACTOR will get paid on a monthly basis upon receiving an accurate account and invoice for service rendered.

i. Prior to submittal, invoices must be certified and signed by a responsible officer of CONTRACTOR with authority to certify that the information submitted by CONTRACTOR is accurate and CONTRACTOR is entitled to payment under the terms of the Contract. COUNTY may rely on said certification in making payment, but this payment will not constitute a waiver of any of COUNTY's legal rights or objections.

ii. If the invoice is in proper form and the items billed are payable under this Contract, COUNTY will make payment to CONTRACTOR.

iii. COUNTY will not be required to make payment if the amount claimed is not in accordance with the provisions of this Contract. All payments under this Contract will be made directly to CONTRACTOR as a corporate entity. Under no circumstances will COUNTY be required to make payments in any amount pursuant to this Contract to any other parties, including individual employees or creditors of CONTRACTOR.

iv. COUNTY is not obligated to reimburse CONTRACTOR for any expenditure not reported to COUNTY within sixty (60) calendar days after the end of the last month of the Contract term.

7. OUTCOME MEASUREMENT REPORTING

This contract requires Social Services Agency's performance and outcome measurement reporting in order to demonstrate the impact of services on client populations. CONTRACTOR shall monitor, measure and report on the service outputs and outcomes outlined in Exhibit H: Logic Model.

CONTRACTOR must submit to COUNTY a quarterly report using the form provided by COUNTY. Instructions and training to complete the form can be found on https://www.youtube.com/watch?v=Ij2VUO4PhW8.

CONTRACTOR must submit the report by the fifteenth (15th) working day after each quarter for services performed during the preceding quarter.

8. ADJUSTMENT TO EXHIBIT B: SCOPE OF SERVICE

A written adjustment to the Scope of Service may be approved by the COUNTY Representative, or designee, identified in this Exhibit, without a contract amendment as long as the adjustment reflects approved original program provisions and both parties are notified at least 10 days before the adjusted Scope of Service begins.

9. ADJUSTMENT TO EXHIBIT H: LOGIC MODEL

A written adjustment to the Logic Model may be approved by the COUNTY Representative, or designee, identified in this Exhibit, without a contract amendment as long as the adjustment reflects approved original program provisions and both parties are notified at least 10 days before the adjusted Logic Model begins.

10. SERVICE PROVIDED

a. CONTRACTOR must inform COUNTY of services and activities performed under this Contract and accept appropriately referred clients from COUNTY for contract services as part of CONTRACTOR's client base.

b. CONTRACTOR must coordinate services with other organizations providing similar services in order to foster community cooperation and avoid unnecessary duplication of services.

11. CONTRACT REPRESENTATIVES

a. CONTRACTOR designates Michael De La Rosa, Chief of Strategic Development as CONTRACTOR's representative for the purpose of performing the services as required by this Contract. Unless otherwise indicated in writing, the above-named person has the primary authority and responsibility to carry out this Contract.

b. COUNTY designates the Director of Social Services Agency, or designee, as its representative for the purpose of managing the services performed pursuant to this Contract.

12. NOTICES

All notices prescribed by this Contract will be in writing and deemed effective if sent by certified mail or registered mail and properly deposited with the United States Postal Service, postage prepaid with return receipt requested and addressed as follows:

a. To COUNTY: Social Services Agency
Office of Contracts Management
333 West Julian Street
San Jose, California 95110-2335

b. To CONTRACTOR: Exemplar Human Services LLC
Andrew Bush, Chief Executive Officer
3511 Bridle Path
Austin, TX, 78703

13. COUNTY'S CONTRACT TRANSITION PROCESS

CONTRACTOR agrees to provide all information deemed necessary by COUNTY for use in subsequent procurement cycles.

CONTRACTOR: Exemplar Human Services, LLC

PROGRAM/PROJECT NAME: Reporting Tools and Services

1. BACKGROUND

The purpose of this Contract is to establish a partnership between COUNTY and CONTRACTOR under which COUNTY-approved staff will receive access to the system for purposes directly connected with the California Statewide Automated Welfare System (CalSAWS) Reporting Tools and Services.

This Contract also sets forth the roles and responsibilities of the parties for the implementation of this partnership.

2. RESPONSIBILITIES OF CONTRACTOR

Pursuant to the purpose of this Contract, CONTRACTOR will fulfill the following responsibilities:

a. Provide Reporting Tools to support all levels of DEBS staff in support of program administration.

3. RESPONSIBILITIES OF SSA

Pursuant to the purpose of this Contract, COUNTY, through DEBS will cooperate with the CONTRACTOR to fulfill the following responsibilities:

a. Provide “read-only” access to the systems client inquiry screens and client correspondence;

b. Provide access to add case comments to the systems as appropriate;

c. Ensure that prior to access of the systems, CONTRACTOR complies with and completes all the requirements as outlined in Section 5 of this exhibit; and

d. Respond to any questions and technical assistance from CONTRACTOR relating to CalSAWS system access including, but not limited to directing concerns to the appropriate agency with the SSA.

4. ACCESS

CONTRACTOR may remotely access COUNTY’s system in compliance with COUNTY’s Request for Access, Remote Access Security Requirements, Privacy and Security Training Disclosure Agreement, and User Responsibility Requirements listed below.

a. Request for CalSAWS’ Access

   1) CONTRACTOR must comply to the data access request process for access to. Compliance to this process is required to ensure appropriate and accurate access is being provided for compliance and security purposes.

   2) CONTRACTOR must complete Exhibit C: System Data Access Request Form and return a completed copy to the COUNTY’s designated Program Monitor.

   3) A written adjustment to Exhibit C may be approved by the COUNTY’s designated Program Monitor, without a contract amendment as long as the adjustment reflects approved original program provisions and both parties are notified at least 10 days before the adjusted request begins.

b. Remote Access Security Requirements

   1) “Remote access” is the act of connecting to COUNTY systems from a non-COUNTY network infrastructure.

   2) All employees of CONTRACTOR working on the systems must ensure compliance with requirements listed on Exhibit D: Contractor Access Security Statement and return a signed copy to the COUNTY’s designated Program Monitor.

c. Privacy and Security Certification Policy

   1) CONTRACTOR must ensure the security and privacy of the client’s Personally Identifiable Information (PII). This Policy will govern all employees, vendors, contractors, community-

based organization and any stakeholders that work for or have an affiliation with, and/or a working relationship with COUNTY and have access to PIIs.

2) It is mandatory for all individuals requiring access to any SSA system to successfully complete the SSA Online Privacy and Security Certification and Training once every twelve (12) months. SSA systems include applications and/or software (collectively referred to as "Toolkit") such as CalSAWS', CalHEERS, MEDS, EBT/EPPIC, BCW, Work Number, SFIS, OCAT, Access CalSAWS', and/or VSAS that contains PIIs AND/OR have opportunity to review/access client's information obtained as a result of access to Toolkit.

3) After completion of the initial certification and training, access will be authorized for one (1) calendar year from the date of completion of training. The SSA Online Privacy and Security training must be completed annually, for the duration of CONTRACTOR's relationship with COUNTY. Upon completion, all employees of CONTRACTOR with access to the Toolkit return a signed copy of Exhibit E: SCCSSA Online Privacy & Security Training Disclosure Agreement to the COUNTY's designated Program Monitor.

4) If individual fails to recertify, their access to the Toolkit will be discontinued at the end of the certification period.

5) If individual is locked out of any system that provides information regarding our client's PII, and/or they have let their certification/training lapsed and/or did not complete the SSA Online Privacy and Security Certification Training, access CANNOT be restored or granted until the certification/training has been successfully completed.

d. CalSAWS' User Responsibility Requirements

1) CONTRACTOR must comply with standards for accessing the SSA information systems and/or networks. CONTRACTOR must also comply with standards for user interaction with information systems and networks attached to. All employees of CONTRACTOR working on the system are personally responsible for knowledge and understanding of these standards and are personally responsible for any actions they take that do not comply with these standards.

2) All employees of CONTRACTOR and SSA's subrecipients working on the systems must ensure compliance with requirements listed on Exhibit F: CalSAWS Information Security Policy and Exhibit G: County Information Technology User Responsibility Statement for Third Parties. A signed copy of said Exhibit must be submitted to the COUNTY's designated Program Monitor.

5. <u>PRIVACY & COMPLIANCE</u>

a. Document retention and destruction provisions in the Contract will apply, as set forth in Exhibit F: County Information Technology User Responsibility Statement for Third Parties.

b. If any of the responses in the future change from the previous SDAR submission, then this request must be re-approved.

c. Permanently delete the data once use of the data is complete.

d. Employee data should be limited to DEBS worker identification number, not employee identification number.

6. <u>SECURITY</u>

a. Data to be shared only via encrypted email (SCCSECURE) or via OneDrive.

b. Any access to County systems remotely must utilize an approved remote method (e.g. SecureLink, Mobile Pass).

c. If an alternative method is proposed, an ISO approval is required.

d. All County data that is deemed sensitive must be encrypted in transit, and at rest, it is based on incurred cost.

e. Any electronic hosting/storing of County data outside County control, other than SalesForce, requires a separate ISO approval process.

f. Required systems access forms must be completed once the CONTRACT is finalized.

7. REPORTING TOOLS & SERVICES

a. CONTRACTOR will produce an Intake Pending Apps Report. This report shall provide a consolidated view of all current pending CalWORKs (CW), CalFresh (CF), Medi-Cal (MC), General Assistance (GA), and Expedited CalFresh (ECF) programs. The report shall contain the following alert indicators: a) Pending CW/CF/MC/GA Applications Due Tomorrow, b) CW App Between 35-45 Days, c) CW App Over 45 Days, d) CW Total Pending, e) CF App Between 20-30 Days, f) CF App Over 30 Days, g) CF Total Pending, h) ECF Due Next Day, i) Overdue ECF, j) MC App Between 35-45 Days, k) MC App Over 45 Days, l) MC Total Pending, m) GA App Between 35-45 Days, n) GA App Over 45 Days, n) GA Total Pending. CONTRACTOR shall provide additional customization as directed by COUNTY.

b. CONTRACTOR will produce a Consolidated Eligibility Report. This report shall be a multiple tab consolidated report representing Eligibility-related information regarding Intake and Continuing eligibility and caseload management tasks. The elements contained in the report shall be: SAR 7 Completion Rate, Overdue Semi-Annual Report (SAR) 7's Previous Month, CW/CF, GA/CF RE Completion Rate, CW/CF, GA/CF RE Current Month, MC RE Current Month, MC RE Current Month Summary, Critical Tasks, and MAGI Overdue Review. CONTRACTOR shall provide additional customization as directed by COUNTY.

1) The SAR 7 Completion Rate report will provide SAR7 information for all CW, CF, GA, GA/CF combination cases, and CW/CF combination cases for the respective SAR 7 Submit Month. The report shall include the following indicators: Program, Total SAR 7's Due, Received, In Sent Status, In Received Status, In Ready to Run Status, Completed, N/A, Incomplete, and Rate. The report will also identify:

   i. If the case has a task with task type of New Hire Run (NHR) set prior to the last completed SAR7/RE, include "(NHR)" next to the Case Number. The NHR task represents a report in CalSAWS that workers must clear.

   ii. Identify and display income amount/types for those CF cases with income that have a SAR 7 reports due.

2) The Overdue SAR 7 report will display any open SAR7s (not 'Complete', 'Incomplete, or 'NA') from the prior submit month received in the current month.

3) The CW/CF, and GA/CF RE Completion Rate report will provide RE information for all CW/CF, and GA/CF cases with RE's due in the respective report month. The report shall include the following indicators: Total CW/CF, and GA/CF RE's Due, In Sent Status, Received, In Received Status, In Ready to Run Status, Completed, N/A, Incomplete, and Rate.

4) The CW/CF, and GA/CF RE Current Month report provides information on CW, GA and CF RE's in Received and Ready to Run status for the respective RE report month. The report shall include the following indicators: Master Assignment Queue (MAQ) Case Number, Case Name, Received On, Last Status Date, Last Status, and Scanned in District. The report will also identify: If the case has a task with task type of NHR set prior to the last completed SAR7/RE, include "(NHR)" next to the Case number. The Master Assignment Queue is used for task-based caseloads when there isn't a single worker assigned.

5) The MC RE Current Month report provides information on MC RE's in Received and Ready to Run status for the respective RE report month. Because the universe for all current month MC REs includes REs that are processed outside of Customer Reports (CR), CONTRACTOR shall identify these as 'RE DUE (NO CR)'. The report shall include the following indicators: MAQ, Case Number, Case Name, Received On, Last Status Date, Last Status, and Scanned in District. The report will also identify: If the case has a task with task type of NHR set prior to the last completed SAR7/RE, include "(NHR)" next to the Case number.

6) The MC RE Current Month Summary report provides summary information on MC RE's in Received and Ready to Run status for the respective RE report month. Because the

universe for all current month MC REs includes REs that are processed outside of Customer Reports (CR), CONTRACTOR shall identify these as 'RE DUE (NO CR)'. The report shall include the following indicators: RE Due (No CR), Ready to Run, Received, Total of Received and RE Due (No CR).

7) The Critical Tasks report Indicates the Task Type of any open Task whose due date has passed or is 1 day out (up to 48 hours) in the future: Felons, Fraud, Aid Paid Pending, State Hearing, Sanction/Penalty, MC 355 Due, Contact Client, and for New Hire Report tasks if created after 5/1/17, (NHR only when associated with a SAR or RE in the respective report month). Also, if there are any open Change Reported tasks where description = C4Yourself, regardless of the end date, it will be included. The report shall include the following indicators: MAQ, Case Number, Task Type, Due Date, and Assign Date.

8) The Modified Adjusted Gross Income (MAGI) Overdue Review identifies MAGI referrals that are in an 'In Process' status 3 or more days after receipt of the referral as indicated on the Referral Date on the MAGI Referral Detail page. The report shall include the following indicators: Received On, In Process Status Date, and Days in Process.

c. CONTRACTOR will produce a Continuing Productivity Report. This report shall be a multiple tab report that provides information on case actions completed by Eligibility Worker staff. The tabs with corresponding information will be Yesterday, Week to Date, and Month to Date for the respective reporting month/timeframe. The report will be customized to identify completed case actions by how they were completed in C-IV, i.e., running Eligibility Determinization and Budget Calculation (EDBC), status updates, etc. The EDBC is the process by which the CalSAWS system determines a client’s eligibility and benefit amount. CONTRACTOR shall provide additional customization as directed by COUNTY.

1) The report shall include the following indicators: SAR 7 Completed, SAR 7 Incomplete, MC RE Completed, MC RE Incomplete, CF RE Completed, CF RE Incomplete, CW RE Completed, CW RE Incomplete, GA RE Completed, GA RE Incomplete, CW/CF RE Completed, CW/CF RE Incomplete, GA/CF RE Completed, GA/CF RE Incomplete, Tasks with SAR 7/RE, Tasks without SAR 7/RE, MEDS Alert with SAR 7/RE, and MEDS Alert without SAR 7/RE.

d. CONTRACTOR will produce an Overtime Productivity Report. This report shall provide information on case actions completed by Eligibility Worker staff during a Saturday overtime session. The tab with this data will appear on the regular Productivity Report on the Monday immediately following the Saturday overtime session. The report will be customized to identify completed case actions by how they were completed in C-IV, i.e., running EDBC, status updates, etc. CONTRACTOR shall provide additional customization as directed by COUNTY.

1) The report shall include the following indicators: SAR 7 Completed, SAR 7 Incomplete, MC RE Completed, MC RE Incomplete, CF RE Completed, CF RE Incomplete, CW RE Completed, CW RE Incomplete, GA RE Completed, GA RE Incomplete, CW/CF RE Completed, CW/CF RE Incomplete, GA/CF RE Completed, GA/CF RE Incomplete, Tasks with SAR 7/RE, Tasks without SAR 7/RE, MEDS Alert with SAR 7/RE, and MEDS Alert without SAR 7/RE.

e. CONTRACTOR will produce a Consolidated Welfare to Work (WtW) Alerts Report. This report shall provide multiple reports, for use by COUNTY WtW staff, into a single consolidated report. CONTRACTOR shall provide additional customization as directed by COUNTY.

1) The WtW Alerts report shall provide information and alerts related to WtW caseload management. It shall include the following indicators: e2Lite, Unengaged, Non-Compliance Over 60 Days, Good Cause Over 30 Days, Activities without Service Arrangements, Activities with No (Null) Attendance, Activities Lingering in Referred Status, Activities Ending in 2 Weeks.

2) The Null Hours Carryover report shall identify cases, that for the respective report month, have had no WtW attendance hours entered for activities from two months ago and prior.

3) The Attendance and Progress report shall provide information on the processing of WtW

733.4 forms by WtW staff. The report shall include the following indicators: Received, Reviewed + Completed, Reviewed + Completed Status Worker ID, and Reviewed Rate.

4) The School Attendance report shall provide information on the processing of WtW 735.2 forms by WtW staff. The report shall include the following indicators: Received, Reviewed + Completed, Reviewed + Completed Status Worker ID, and Reviewed Rate.

5) The Travel Claims Completion Rate report shall provide information on the processing of WtW 753A forms by WtW staff. The report shall include the following indicators: Claims Received, Claims Reviewed + Completed, Reviewed + Completed Status Worker ID, Claims Reviewed/Completed Rate.

6) The Travel Claims Carryover report shall Indicate the 753A forms received in a prior month, from the respective report month, that have never been reviewed in any way (Reviewed, Incomplete, NA, Denied, Error).

7) The Travel Claims NA or Incomplete report shall identify 753A forms in the respective report month that have never been in a completed status and are currently in either NA or IN status.

8) The Child Care Alerts report shall provide alerts related to the Child Care program. The report shall include the following indicators: Child Care Applications Coming Due, Overdue Child Care Applications, IDT, Over 47 Months, Tasks Coming Due, Tasks Overdue, 12 Years + 11 Months and Older, and No Payments Issued in Last Three Periods.

9) The Child Care Reimbursement Completion Rate report shall provide, for the respective report month, information on the processing of Child Care Resource and Referral (CCRR) 100 forms by WtW and Fiscal staff. The report shall include the following indicators: Received, Reviewed, Reviewed Status Worker ID, Reviewed Rate, Payment Issued, and Payment Issued Rate.

10) The Carryover-Received Not Reviewed report shall identify those CCRR 100 forms, from a month prior to the respective report month, that are in a Received status and have not been updated to a Reviewed status.

11) The Carryover-Reviewed, No Payment report shall identify those CCRR 100 forms, from a month prior to the respective report month, that are in a Reviewed status and have not had a payment issued.

f. CONTRACTOR will produce an Office Assistant Productivity Report. This report shall be a multiple tab report that provides information on clerical actions completed by Office Assistant staff. The tabs with corresponding information will be Yesterday, Week to Date, and Month to Date for the respective reporting month/timeframe. The report will be customized to identify completed clerical actions by how they were completed in C-IV, i.e., status updates. CONTRACTOR shall provide additional customization as directed by COUNTY.

1) The report shall include the following indicators: Apps Pended, REAC's Completed, EBT Cards Issued, Gas Cards Issued, Bus Passes Issued, Vouchers Issued, Travel Claims Processed, HA Payments Processed, and Diaper Issuances Processed.

g. CONTRACTOR will produce an Office Assistant Overtime Productivity Report. This report shall provide information on clerical actions completed by Office Assistant staff during a Saturday overtime session. The tab with this data will appear on the regular Office Assistant Productivity Report on the Monday immediately following the Saturday overtime session. The report will be customized to identify completed case actions by how they were completed in C-IV, i.e., status updates. CONTRACTOR shall provide additional customization as directed by COUNTY.

1) The report shall include the following indicators: Apps Pended, REAC's Completed, EBT Cards Issued, Gas Cards Issued, Bus Passes Issued, Vouchers Issued, Travel Claims Processed, HA Payments Processed, and Diaper Issuances Processed.

h. CONTRACTOR will produce an Application Productivity Report. This report shall provide monthly application productivity data for CW, CF, MC, and FC. Information shall include application disposition and timeliness data. CONTRACTOR shall provide additional customization as directed by COUNTY.

i. CONTRACTOR will produce a Productivity Tele-work Comparison Report. This report shall display the comparison of work completed of staff while in DEBS offices as compared to work completed on their tele-workdays.

j. CONTRACTOR will produce a WtW Productivity Report. This report shall provide information on work completed by WtW staff. CONTRACTOR shall provide additional customization as directed by COUNTY.
k. CONTRACTOR will produce an Executive Dashboard. This report shall be a monthly summary of key performance metrics of the DEBS. Metrics can include application processing, application disposition, renewal processing, SAR processing, application counts, program counts, program discontinuances, etc.
l. CONTRACTOR will provide agreed upon reports in Microsoft Power Business Intelligence (PBI).
m. CONTRACTOR will produce all reports in Microsoft Excel, unless otherwise directed by COUNTY.
n. CONTRACTOR will distribute reports to COUNTY staff by email, unless otherwise directed by COUNTY.
o. CONTRACTOR will provide color coding, highlighting, shading or other means of identifying lingering cases on reports or for any other purposes as directed by COUNTY.
p. CONTRACTOR will ensure all reports shall be produced in a drill down format, with comparative views between regions, offices, units, and workers, unless otherwise directed by COUNTY.
q. COUNTY shall have the right to request modifications to any of the reports.
r. CONTRACTOR shall resolve any data investigation issue within one business day from receipt of issue from COUNTY.
s. CONTRACTOR shall receive up to five new reports per quarter at no charge.
t. CONTRACTOR shall provide ad-hoc reporting services to the COUNTY.
u. COUNTY shall have unlimited users with access to reporting tools and services.
v. All reporting tools and services shall be delivered daily, unless otherwise directed by COUNTY.

Santa Clara County
Social Services Agency

FY 2024-2025

Exhibit B: Scope of Service
Staffing
Page 1 of 1

Contractor:	**Exemplar Human Services, LLC**
Contract Period:	**Upon execution - June 30, 2025**
Program:	**Reporting Tools and Services**

Provide the following information for each staff member who would be assigned to fulfill the terms of contract.

#	Staff Job Title	Activities Staff Person Will Perform	Education, Experience, and Qualifications	Language and Cultural Competence
1	Chief of Strategic Development	Contract monitoring, client relations, technical assistance, program support, meeting with Santa Clara staff.	Bachelor's Degree in Business Administration, 19 years of County human services experience, 9 years of experience with Exemplar Human Services	
2	Lead Technical Architect	Data connection, data design and build. Reports design and build. Ongoing report monitoring and review. Technical and quality control monitoring.	Bachelor's Degree, more than 20 years of IT experience, extensive knowledge of CalSAWS design, multi-faceted knowledge of technology, including software, hardware, systems, connections, etc.	
3	Data Warehouse Developer	Data mining and research, data development for business intelligence reporting aka Exemplar reporting. Along with the maintenance, updates, or enhancement of said reports, and daily processes.	Associate's Degree, approximately 20 years in Business Intelligence, data warehousing, data and report development across multiple platforms.	
4	Database Analyst	Creation of reports, creation of ad-hoc reports, quality control activities, feasibility reviews and data investigations.	Bachelor's Degree in Statistics, 20 years of .spl experience, expert on CalSAWS schema and functionality, very familiar with CDSS policy and County processes.	
5				
6				
7				

Exhibit C

Contractor Access Security Statement

Agreement Between Contractor: Exemplar Human Services, LLC and County of Santa Clara Department of Employment & Benefit Services

1. Definitions

a. "Remote Access" is the act of accessing County Systems from a non-County network infrastructure.

b. "County Systems," for purposes of this Exhibit, include but are not limited to, all County-owned, leased or managed servers, mainframe computers, desktop computers, laptop computers, handheld devices (including smart phones, wireless PDAs and Pocket PCs), equipment, networks, application systems, databases, software, phone systems, any device with network capabilities (e.g., a workstation with an attached modem, routers, switches, laptop computers, handheld devices), and any other system that stores, processes, and/or transmits County-owned information/data. These items are typically under the direct control and management of the County. "County Systems" also include these items when they are under the control and management of a service provider for use by County, as well as any personally-owned device that an individual has express written permission to use for County purposes.

c. "County-owned information/data," for purposes of this Exhibit, is any information or data that is transported across a County network, or that resides in a County-owned information system, or on a network or system under the control and management of a service provider for use by County. This information/data is the exclusive property of County unless constitutional provision, State or Federal statute or case law provide otherwise. County-owned information/data does not include a User's personal, non-County business information, communications, data, files and/or software transmitted by or stored on a personally-owned device if that information/data is not transported across a County network or does not reside in a County System or on a network or system under the control and management of a service provider for use by County.

d. "Contractor employees" includes Contractor's employees, agents, representatives, contractors or subcontractors performing services under this Agreement.

2. Scope of Access

a. County grants Remote Access privileges (through the method described in section 9) for Contractor to access the following County Systems (collectively referred to as "Designated Systems"), in accordance with the terms of this Agreement:

County System: California Work Opportunity and Responsibility to Kids Information Network (CalSAWs)

b. All other forms of access to the Designated Systems, or to any County System that is not specifically named, is prohibited.

Exhibit C

c. Remote Access is granted for the purpose of Contractor providing services and performing its obligations as set forth in this Agreement including, but not limited to, supporting Contractor-installed programs. Any access to the Designated Systems, County-owned information/data, or any other County System or asset that is not specifically authorized under the terms of this Agreement is prohibited and is a material breach that may result in immediate termination of this Agreement for cause and any penalty allowed by law. Contractor may only access the Designated Systems

d. County will review the scope of Contractor's Remote Access rights periodically.

3. Security Requirements

a. Contractor will not install any Remote Access capabilities on any County System unless such installation and configuration is approved by the County Information Security Office and meets or exceeds NIST 800-53 standards, or an equivalent industry standard.

b. Contractor will only remotely access Designated Systems, including access initiated from a County System, if the following conditions are met:

1) Upon request by an authorized County representative, Contractor will submit documentation verifying its own network security mechanisms to County for County's review and approval. The County reserves the right to advanced written approval of Contractor's security mechanisms prior to Contractor being granted Remote Access.

2) The Remote Access method agreed upon pursuant to paragraph 9 must include the following minimum control mechanisms:

a) Two-Factor Authentication: An authentication method that requires two of the following three factors to confirm the identity of the user attempting Remote Access. Those factors include: 1) something you possess (e.g., security token and/or smart card); 2) something you know (e.g., a personal identification number (PIN)); or 3) something you are (e.g., fingerprints, retina scan). The only exceptions are County approved County-site-to-Contractor-site Virtual Private Network (VPN) infrastructure.

b) County personnel will control authorizations (permissions) to specific systems or networks.

c) All Contractor systems used to remotely access County Systems must have industry-standard anti-virus and other security measures that might be required by the County (e.g., software firewall) installed, configured, and activated.

4. Monitoring/Audit

County will monitor access to, and activities on, County Systems, including all Remote Access attempts. Data on all activities will be logged on a County System and will include the date, time, and user identification.

5. **Copying, Deleting or Modifying Data**

Contractor is prohibited from copying, modifying, or deleting any data contained in or on any County System unless otherwise stated in this Agreement or unless Contractor receives prior written approval from County. This does not include data installed by the Contractor to fulfill its obligations as set forth in this Agreement.

1. **Connections to Non-County Networks and/or Systems**

Contractor agrees to make every effort to protect data contained on County Systems within Contractor's control from unauthorized access. Prior written approval is required before Contractor may access County Systems from a non-designated system. Such access will use information security protocols that meet or exceed NIST 800-53 standards, or an equivalent industry standard. Remote Access must include the control mechanisms noted in Paragraph 3(b)(ii) above.

2. **Remote Access Contacts**

The following persons are points of contact for purposes of this Exhibit:

Contractor: **Michael De La Rosa**
Chief of Strategic Development
Exemplar Human Services LLC
200 S. Virginia St, Ste 80061, Reno, NV 89501
Phone #: (909)731-4779
Email Address: mdelarosa@exemplarhs.com

County: **Heather Mitchell**
CalSAWs/ Manager
Santa Clara County Program Support, Research and Evaluation
353 W Julian St. 6th Floor, San Jose CA 95110-2335
Phone #: 408-755-7508
Email Address: Heather.Mitchell@ssa.sccgov.org

Either party may change the aforementioned names by providing the other party with no less than three (3) business days prior written notice.

3. **Additional Requirements**

Contractor agrees to the following:

a. Only Contractor employees providing services or fulfilling Contractor obligations under this Agreement will be given Remote Access rights.

b. Any access to Designated Systems, other County Systems and/or County-owned information/data that is not specifically authorized under the terms of this Agreement is prohibited and is a material breach that may result in immediate termination of the Agreement for cause and any other penalty allowed by law.

c. An encryption method that meets or exceeds Federal Information Processing Standard (FIPS) Publication 140-2 will be used.

d. Contractor shall protect the integrity of County Systems and County-owned information/data while remotely accessing County resources, and shall report any suspected security incident or concern to the County Service Desk within 24 hours: (408) 970-2222 or support@tss.sccgov.org.

e. Contractor shall ensure compliance with the terms of this Exhibit and the Exhibit on County Information Technology User Responsibility Statement for Third Parties by all Contractor employees performing services under this Agreement.

f. Contractor employees have no right, or expectation, of privacy when remotely accessing County Systems or County-owned information/data. County may use audit tools to create detailed records of all remote access attempts and remote access sessions, including User identifier, date, and time of each access attempt.

g. Contractor employees that have been provided with a County-owned device intended for remote access use, such as a laptop or other Mobile Device, shall ensure that the device is protected from damage, access by third parties, loss, or theft. Contractor employees shall report loss or theft of such devices to the County Service Desk within 24 hours: (408) 970-2222 or support@tss.sccgov.org.

4. Remote Access Methods

a. All forms of Remote Access will be made in accordance with mutually agreed upon industry standard protocols and procedures, which must be approved in writing by the County. The remote access solution must conform to County policy and security requirements.

b. Remote Access Back-Up Method may be used in the event that the primary method of Remote Access is inoperable.

c. Contractor agrees to abide by the following provisions related to the Primary and (if applicable) Backup Remote Access Methods selected below. (Please mark appropriate box for each applicable Remote Access Method; if a method is not applicable, please check the button marked N/A).

1) **VPN Site-to-Site** ● **Primary** ○ **Backup** ○ **N/A**

The VPN Site-to-Site method involves a VPN concentrator at both the Contractor site and at the County, with a secure "tunnel" opened between the two concentrators. If using the VPN Site-to-Site Method, Contractor support staff will have access to the Designated Systems from selected network-attached devices at the Contractor site.

2) **VPN Client Access** ○ **Primary** ● **Backup** ○ **N/A**

In the VPN Client Access method, a VPN Client (software) is installed on one or more specific devices at the Contractor site, with Remote Access to the County (via a County VPN concentrator) granted from those specific devices only.

An Authentication Token (a physical device or software token that an authorized remote access user is given for user authentication purposes, such as a CryptoCard, RSA token, SecureAuth IdP, Arcot software token, or other such one-

Exhibit C

Contractor Access Security Statement

time-password mechanism approved by the County Information Security Office) will be issued to the Contractor in order to authenticate Contractor staff when accessing County Designated Systems via this method. The Contractor agrees to the following when issued an Authentication Token:

a) Because the Authentication Token allows access to privileged or confidential information residing on the County's Designated Systems, the Contractor agrees to treat the Authentication Token as it would a signature authorizing a financial commitment on the part of the Contractor.

b) A hardware Authentication Token is a County-owned physical device, and will be labeled as such. The label must remain attached at all times.

c) The Authentication Token is issued to an individual employee of the Contractor and may only be used by the designated individual.

d) The Authentication Token must be kept in the possession of the individual Contractor employee it was issued to or in a secured environment under the direct control of the Contractor, such as a locked office where public or other unauthorized access is not allowed.

e) If the Contractor's remote access equipment is moved to a non-secured site, such as a repair location, the Authentication Token will be kept under Contractor control.

f) If the Authentication Token is misplaced, stolen, or damaged, the Contractor will notify the County TechLink Center by phone within 24 hours.

g) Contractor agrees to use the Authentication Token as part of its normal business operations and for legitimate business purposes only.

h) The Authentication Token will be issued to Contractor following execution of this Agreement. Hardware Authentication Tokens will be returned to the County's Tech Link Center within five (5) business days following contract termination, or upon written request of the County for any reason.

i) Contractor will notify the County's the County TechLink Center within one working day of any change in personnel affecting use and possession of the Authentication Token. The County Service Desk contact information is (408) 970-2222 or support@tss.sccgov.org. Contractor will obtain the Authentication Token from any employee who no longer has a legitimate need to possess the Authentication Token. The County will recoup the cost of any lost or non-returned hardware Authentication.

j) Contractor will not store account or password documentation or PINs with Authentication Tokens.

k) Contractor will ensure all Contractor employees that are issued an Authentication Token will be made aware of and provided with a written copy of the requirements set forth in this Exhibit.

3) County-Controlled VPN Client Access ○ **Primary** ○ **Backup** ● **N/A**

This form of Remote Access is similar to VPN Client access, except that the County will maintain control of the Authentication Token and a PIN number will be provided to the Contractor for use as identification for Remote Access purposes.

When the Contractor needs to access County Designated Systems, the Contractor must first notify the County's Remote Access Contact.

The County's TechLink Center will verify the PIN number provided by the Contractor. After verification of the PIN the County's designee will give the Contractor a one-time password which will be used to authenticate Contractor when accessing the County's Designated Systems. Contractor agrees to the following:

a) Because the PIN number allows access to privileged or confidential information residing on the County's Designated Systems, the Contractor agrees to treat the PIN number as it would a signature authorizing a financial commitment on the part of the Contractor.
b) The PIN number is confidential, County-owned, and will be identified as such.
c) The PIN number must be kept in a secured environment under the direct control of the Contractor, such as a locked office where public or other unauthorized access is not allowed.
d) If the Contractor's remote access equipment is moved to a non-secured site, such as a repair location, the PIN number will be kept under Contractor control.
e) The PIN number can only be released to an authorized employee of the Contractor and may only be used by the designated individual.
f) If the PIN number is compromised or misused, the Contractor will notify the County's designee within one (1) business day.
g) Contractor will use the PIN number as part its normal business operations and for legitimate business purposes only. Any access to Designated Systems, other County Systems, and/or County-owned information/data that is not specifically authorized under the terms of this Agreement is prohibited and is a material breach that may result in immediate termination of the Agreement for cause and any other penalty allowed by law.
h) The PIN number will be issued to Contractor following execution of this Agreement.
i) The PIN number will be inactivated by the County's designee within five (5) business days following contract termination, or as required by the County for any reason.

4) County-Controlled Enexity Access ○ **Primary** ○ **Backup** ● **N/A**

The County-Controlled Enexity Access method involves using Securelink's Enexity tool installed in the County. County will establish a gateway where Contractor can access the Designated Systems from selected network-attached devices at the County site. County will control the access list for Contractors with access through Enexity gateways.

Signatures of Contractor Employees receiving Authentication Tokens (**<u>Only for VPN Client Access and if tokens issued by County</u>**):

Exhibit C

Contractor Access Security Statement

SIGNATURE:____ [TYPE NAME AND TITLE HERE.]
Date: _____________________________________

SIGNATURE:____ [TYPE NAME AND TITLE HERE.]
Date: _____________________________________

SIGNATURE:____ [TYPE NAME AND TITLE HERE.]
Date: _____________________________________

SIGNATURE:____ [TYPE NAME AND TITLE HERE.]
Date: _____________________________________

Exhibit D

Santa Clara County Social Services Agency
Online Privacy and Security Training Disclosure Agreement

Please Print

Under the penalty of perjury, this document certifies that I,

Last Name: ______________________________ First Name: __________________________

Physical Work Address: ____

Work Telephone Number: ____

Email Address: ____

I am an employee or representative of (Name of Organization):

Organization Address (if different from above Work Address):

____

I have completed the Social Services Online Privacy and Security Training as required by the County of Santa Clara. And will comply with the information set forth in said training.

By signing this form, I further understand my civil liability, that in addition to being guilty of a misdemeanor, a person responsible for unauthorized, negligent disclosure of confidential information may expose himself to civil liability and the client who is damaged by such a disclosure may bring suit against the person.

Date Successfully Completed Training: _______________________ Last 4 digits of SSN or 4 digit PIN: _______

Location: https://360.articulate.com/review/content/62779dfa-3d24-4637-bff8-dfaeca3df3be/review

I understand that I must complete this training annually as required, and that my access to programs supported by Santa Clara County Social Services Agency CalSAWs Application Triage and Support (CATS) will be terminated in one year from the date of successful completion of training if I do not comply.

Signature:______________________________Title: ___________________________________

Date: _______________________

FOR COUNTY USE ONLY

Received by: ____

Date Received: ____

Exhibit E

CalSAWS Information Security Policy

Purpose

This policy contains security measures for properly developing, administering, and managing systems, including operating systems, databases, applications, and network devices. The purpose of this policy is to provide a comprehensive set of security requirements to ensure protection of sensitive CalSAWS, client, and third-party information entrusted to CalSAWS or to which access is otherwise available.

Compliance

Notice of Compliance

Security is the responsibility of everyone accessing CalSAWS systems and data. The security measures described herein define the basic minimum level of security required for CalSAWS systems and information. Non-compliance with the required security measures and behaviors outlined in this policy could pose significant business and legal risk to CalSAWS and may create a potential for legal actions that could significantly impact CalSAWS's operations and damage its business assets and reputation. Therefore, compliance with this policy, as well as all other CalSAWS security-related policies, is mandatory for CalSAWS personnel, as well as any third parties (such as outsourcing providers, contractors, alliance partners, clients, etc.) that access CalSAWS systems or data. No one is permitted to bypass the security mechanisms provided by CalSAWS systems or infrastructure for any reason. Failure to comply with this policy will be reported and disciplinary action may be taken. Such action may include, but is not limited to, reprimand, financial penalties, termination of employment, and/or legal action.

Precedence

This policy does not replace existing County policies. Rather, this policy is intended to augment existing County policies. To maximize the security of CalSAWS data, where there is a conflict between this policy and an existing County policy, if possible, every effort will be made to adjust the CalSAWS policy to reflect the stronger of the two. If this is not possible, an exception will be noted in this document. Where a County policy is silent on a subject addressed by this policy, this policy will take precedence.

Exceptions, Migration, and Timeframes

Any exceptions to this policy must be clearly documented and submitted to the CalSAWS Systems Security Officer for approval.

All CalSAWS systems must comply with the statements in this policy as soon as possible, not to exceed one year from the time of publication.

Scope

Unless otherwise stated, this policy applies to the security of all workstations, servers, databases, network devices, and applications within all CalSAWS environments (including production, testing, and development), as well as to the information contained on those resources. This policy also applies to mobile devices and home computers and networks to the extent that they store or process CalSAWS data.

Exhibit E

In Scope

The following security elements, users, and systems are in scope for this Policy.

Security Elements

- Identification (e.g., user ID) and Authentication (e.g., passwords and/or PINs)
- Authorization (e.g., access roles and access control)
- Confidentiality (e.g., encryption), Integrity (including system, data and message integrity), and Availability
- Accountability (e.g., tracking and audit) and Non-Repudiation

Users

- All CalSAWS personnel, including administrators and Help Desk personnel
- All County personnel requiring access to CalSAWS resources (e.g., computers, networks, applications, data), including, collaborators, super-collaborators, County Managed Users (CMUs), and Non-Managed Users (NMUs)

Systems

- CalSAWS networks and their components
- Home or personal networks and systems when connected to CalSAWS networks, or if using/storing CalSAWS data
- CalSAWS systems on networks other than the CalSAWS network
- Non-CalSAWS systems storing or processing sensitive CalSAWS data (e.g., collaborator or home systems)
- CalSAWS development and test environments

Out of Scope

The following security elements, users, and systems are considered out of scope of this Policy.

Security Elements

- Confidentiality (e.g., encryption) of welfare recipient data when not on a CalSAWS system.
- Data and message integrity for welfare recipient information when not on a CalSAWS system.

Users

- Any personnel that do not have access to CalSAWS resources.
- Individuals accessing CalSAWS's publicly available Internet websites (on www.c-iv.org) that are not CalSAWS personnel, nor county employees.

Systems

- Home or personal networks and systems when not connected to CalSAWS networks or using/storing sensitive CalSAWS data
- Collaborator system or networks when not connected to CalSAWS networks or utilizing sensitive CalSAWS data.

Exhibit E

Roles and Responsibilities

The CalSAWS Systems Security Officer is responsible for the day-to-day management of CalSAWS security matters. The Systems Security Officer will seek guidance from the CalSAWS Project Director, members of the Consortium, the Security Advisory Committee, and when necessary, the Joint Powers Authority (JPA) Board, all of whom are responsible for making strategic security decisions as they apply to CalSAWS. The Systems Security Officer will also have access to various technical resources (e.g., system administrators, network administrators, database administrators, application development personnel, etc.), who are responsible for participating in ad-hoc Security Teams to handle incidents, manage disasters, and investigate possible intrusions. All CalSAWS personnel are responsible for complying with policies and assisting the Systems Security Officer as required.

Volume I of the System Operations and Support Plan (SOSP) provides detailed role descriptions for the above-mentioned individuals.

Identification

Identification is the process that enables recognition of the user by the specific system. This section focuses on the policy for creation and maintenance of IDs for CalSAWS personnel, county users, Collaborators, Super-Collaborators, and applications.

IDs for CalSAWS Personnel

In the context of this policy, CalSAWS personnel are defined as individuals working on the CalSAWS Project in the CalSAWS Production Data Center (PDC), Development Data Center (DDC), Network Operations Center (NOC), Project Management Office (PMO) and Application Development Facility (ADF). Each such individual must be assigned his or her own unique ID, which will be linked to the individual’s name, personnel number, or other unique, CalSAWS-approved identifier, to provide accountability.

Only CalSAWS personnel who require administrative privileges will be assigned such. Individual IDs will be assigned the necessary administrative capabilities so that CalSAWS Administrators may carry out their assigned job functions. Administrators will not share the Windows *Administrator* account. The Windows *Administrator* account will be renamed to a common username, and individual IDs will be created with the necessary privileges for each Windows administrator. Administrators will not directly access the *root* account in the UNIX environment. The use of the UNIX “su” command or other similar mechanism is mandatory in UNIX environments to enable accountability with the root account.

Having an ID containing both user and administrative privileges is discouraged, due to the possibility of accidental systems damage that may occur as a result of an individual trying to execute user tasks with elevated access. Therefore, where possible (e.g., for UNIX server administrators, database administrators, etc.), individuals requiring both administrator and end user access should have separate administrator IDs, different from the non-privileged account IDs. However, since duplicate IDs are also discouraged, individuals needing both user and administrative privileges on an Active Directory integrated system (e.g., Windows 2000, CalSAWS web applications, etc.) will likely have user and administrative privileges attached to a single ID. In such cases, extreme care must be taken when executing user tasks, to ensure that the system is not inadvertently compromised.

Exhibit E

County User, Collaborator, and Super-Collaborator IDs

Each county user must be assigned a unique user ID, which will be linked to the user's name, personnel number, or other unique, county-approved identifier, to ensure accountability.

Each collaborating organization must be assigned a unique Collaborator ID, which will be linked to the organization's name. Since Collaborators only provide and update public information, Collaborator IDs may be shared by up to three individuals within one collaborating organization. The sharing of Collaborator IDs across collaborating organizations is strictly prohibited.

A Super-Collaborator is an individual from a Collaborating organization that has privileged access, instead of the normal Collaborator access as described above. Each Super-Collaborator must have his or her own unique Super-Collaborator ID, with appropriate access controls. Since Super-Collaborators can access and update sensitive CalSAWS data, the sharing of Super-Collaborator IDs between individuals or organizations is strictly prohibited.

All county user IDs and Collaborator IDs will follow the standard naming convention described in Volume I of the CalSAWS SOSP.

Application IDs

Each CalSAWS application and legacy application interacting with CalSAWS systems must be assigned a unique application ID that clearly identifies that application. The same application ID may be used to access multiple systems, but multiple applications cannot share the same application ID, nor may human users utilize an application ID to access systems.

Application ID names must be created such that the function of that account is clear. Application IDs must be easily distinguishable from user IDs (e.g., by using the string 'app' in the application ID name, or by including the application name in the ID).

Vendor Firefighter IDs

Vendor Support Teams often require access to the CalSAWS System in order to assist the CalSAWS Operations Team in diagnosing and troubleshooting an issue. These Vendor Support teams are given an existing Vendor Firefighter ID. The Vendor Firefighter ID is specific to the vendor, but not to a specific vendor employee. These IDs are activated at the time of need and deactivated once the problem is resolved. The password is also changed at the time of deactivation. The activating and deactivating of a Vendor Firefighter ID shall be documented in a CA Service Desk Manager Change Order. This Change Order should reference the Unicenter Request that documents the issue to be investigated. The following must be documented in the Unicenter Change Order: business need for issue of ID, date and time of access given, and vendor contact information. This Change Order will need to obtain the same approval as all Unicenter Change Orders. As per existing process, an access log of alla activity will be kept. The access will be logged as part of existing logging of system actions.

Project Firefighter IDs

Firefighter IDs for project members requiring elevated access will follow the same process as Vendor Firefighter IDS. Instead of Vendor contact information, employee contact information will be documented in the Unicenter Change Order.

Shared IDs

A shared ID is any administrator, application, or user ID that is used by multiple people and/or applications. Shared IDs severely decrease or eliminate accountability on the system. As such,

Exhibit E

creation and use of shared IDs, with the exception of Collaborator IDs and Vendor Firefighter IDs as described above, is strictly prohibited on CalSAWS systems that contain Production Data.

Authentication

CalSAWS administrators and applications must follow the authentication requirements detailed below.

Password Authentication

The following sections provide general guidelines that should be adhered to when creating and maintaining passwords. Note: The UNIX environment technology does not support all the password rules documented in this section. In the case of the UNIX environment, the password rules will meet the general password rules to the extent that the current hardware/software technology employed in the CalSAWS environment allows.

Note: The Solaris operating systems do not allow for the creation/maintenance of users' ID's and Password uniqueness as specified for the CalSAWS application and Active Directory IDs. As a result, MINWEEKS, MAXWEEKS, and WARNWEEKS are not set at all. The only requirement in place is PASSLENGTH=8.

Note: Within the CalSAWS Active Directory environment the Counties which support Novell as the primary Network operating system have requested that CalSAWS not enforce complex passwords requirement. All the other County domains enforce a max password of 60 days.

Password Strength

Passwords must meet certain length and complexity requirements to protect the data being accessed. Systems will be configured to require passwords that are at least eight characters long, and meet three of the four complexity categories (i.e., upper-case letters, lower-case letters, numerals, and non-alphanumeric symbols). Null (i.e., blank) passwords are strictly prohibited. Initial user passwords may be alphanumeric only but must be configured to expire after a single use.

Password strength rules will be the general norm for password creation regardless of the system's ability to enforce them.

Password Age

Passwords must meet maximum age requirements to ensure the continued integrity of each password. Unless noted above, Systems will be configured to expire administrator and user passwords at least every 60 days, and application passwords at least every 180 days. User passwords must also meet minimum age requirements.

Application passwords must be manually changed when an administrator who knew the password leaves the group (i.e., changes role or leaves CalSAWS).

Password age rules will be the general norm for password creation unless noted above.

Password Uniqueness

Newly created passwords must be significantly different from previous passwords to ensure the continued integrity of CalSAWS systems. Unless noted above, systems will be configured to prevent the reuse of any password within a period of one year since the last use.

Exhibit E

Note: Most systems represent password history as a number of passwords to remember, rather than time since last usage. The password history value (i.e., number of passwords remembered) shall be calculated to ensure that passwords are not reused for a period of one year, based on the expiration frequency

To ensure the uniqueness of system passwords, no system password will be the same as or similar to the default passwords provided at system setup, and no two types of system will have the same system password.

Password uniqueness rules will be the general norm for password creation unless noted above.

Account Lockout

Unless noted above, systematic controls must be in place to limit the number of times a user or application can unsuccessfully authenticate with the system. After a user or application has incorrectly entered a password 5 times in a row, the account must be locked out such that the user must contact their local Help Desk for assistance. Account lockout counters will reset after a period of 30 minutes. Administrator accounts will not have lockout capabilities enabled.

Locked Collaborator passwords will not be unlocked; the Collaborator’s password will be reset, and a temporary password sent to the Collaborator’s registered email address. The temporary password will be good for the initial access only and must be changed at first login.

Password Protection

Due to the number and complexity of administrator passwords, administrators may write down the first half of the password if needed but must keep the paper on which the password fragments are written in a locked drawer or similarly secure location. If an administrator believes that his or her password has been compromised, s/he must report the incident immediately to their supervisor and to the Systems Security Officer and change all passwords that were documented. Under no circumstances may any administrator share their passwords with others.

Applications (e.g., batch scripts) that need to interact with other systems that require authentication must not store passwords inside of the application (i.e., ‘hard-coded’ passwords within the script). Application passwords must be encrypted and stored in a system-protected password file that can be accessed as needed by the application, and only by the application.

Passwords must be actively entered each time they are requested and may not be stored on the local machine. Under no circumstances may any administrator or application passwords be saved using the ’save password to this machine’ or ’remember my password on this computer’ mechanism that is offered by Windows and many vendor applications.

Event-Based Authentication

Individuals’ access rights to CalSAWS data change over time as their roles change within CalSAWS or as they leave the organization. Therefore, a user’s identity and authority to access data must be reconfirmed at the time data is accessed. It is not sufficient to grant ongoing access to CalSAWS data based on a user’s status at the time of registration. Credentials not controlled by CalSAWS (including, but not limited to, instant messaging accounts, external email addresses, and external certificates) may not be used to grant access to sensitive CalSAWS data.

Exhibit E

Bypassing Authentication Mechanisms

The use of mechanisms that bypass authentication (e.g., .rhosts and .netrc files in UNIX, pass-through authentication in Windows) is strictly forbidden within the CalSAWS environments. Mechanisms that bypass the standard authentication method maximize the damage in the event of a security incident.

Access Control

Access to information and information resources must be properly authorized and must be appropriate to the value of the information to CalSAWS, considering the potential and consequences of loss or misuse of the information. This section outlines the access control rules for CalSAWS.

Inactivity Timeouts

Any computer that can access CalSAWS systems or data must be configured to invoke a password-protected screensaver on its monitor after no more than 10 minutes of inactivity.

Systematic controls must be put in place to require users, administrators, and applications to re-authenticate with the system after a given amount of inactivity. The timeout period for users, administrators, and applications will vary according to the sensitivity of data accessed.

Account Inactivity

Enabled but unused accounts can provide a means of access to unauthorized users. If technically possible, systems will be configured to automatically disable any account that has not been used for a minimum of one month.

Access Roles

Within each application or system, Role-Based Access Control will be enforced. That is, for any given application or system, each CalSAWS job function will have its own distinct access role, to which a given set of system or application permissions shall be assigned. All individuals and/or applications having the same job function will have the same access role(s). The Least Privilege Principle will be applied: no individual or application may have more access than is required to perform the assigned job function(s). An individual or application may have multiple access roles.

Creating New Access Roles

If an administrator, application, or user requires a permission that cannot be accommodated by an existing access role (i.e., existing roles contain too many or too few permissions), a new access role will be created to accommodate the need. The creation of a new access role must undergo a change control process and must be approved by the Systems Security Officer (for CalSAWS systems) or an authorized County representative (for county functional users).

Maintaining and Auditing Access Control

A list of current CalSAWS access roles will be maintained by each County or system owner or manager, and CalSAWS personnel, county users, collaborators, super-collaborators, and applications will be assigned one or more access roles, based on their job function(s). Systematic controls must be in place to regularly verify synchronization between people, applications, and their access roles. Where the system does not support this, manual checks

Exhibit E

must be made to verify synchronization between users, administrators, applications, and their access roles.

Activation and Deactivation of Access

To provide that access is properly assigned, permissions may only be enabled, disabled or changed by authorized personnel responsible for user management, or by automated systems according to approved business rules. Access will not be enabled, disabled, or changed unless the request was submitted by an authorized requestor. Personnel and systems that are responsible for managing user access must know who or what is authorized to make such requests.

CalSAWS access must be revoked immediately upon termination of personnel, or when an individual changes role and ceases to need existing access.

Collaborator Access

The CalSAWS System provides collaborators with access to view and update certain data for business activities through established partnerships. Use of CalSAWS resources for purposes other than County business is prohibited. The following requirements apply to CalSAWS Collaborators:

- Collaborators are authorized to communicate services available and perform non-sensitive data updates only
- Collaborator organizations must identify the CalSAWS Project information to which they need access and the reason for access and/or update capability
- Each collaborating organization must first register as an active service organization and provide the following identifying information: organization name, contact name, postal service address, email address, and phone number.

Access to County Legacy Systems

CalSAWS Personnel are strictly prohibited from accessing County legacy systems through CalSAWS systems, unless such access is explicitly granted by the County for authorized purposes.

Physical Security

All CalSAWS central facilities that house CalSAWS servers or data (i.e., PDC, DDC, NOC, and ADF) will have, at a minimum, basic physical security measures to protect CalSAWS systems. CalSAWS systems will be stored in locked rooms with floor-to-ceiling walls. Doors to the server room will have an auditable entry mechanism (e.g., card reader) that records who enters and leaves.

Only authorized personnel will have access to server rooms. Vendors and guests must be escorted by an authorized person while in the Data Center and must sign in and out in a written log. Log details will include the individual’s name, time entering the Data Center, time leaving the Data Center, and reason for visit.

During non-working hours, secure areas at the DDC, PDC, NOC, and ADF shall be protected against intrusion by appropriate surveillance systems and/or security staff. In the event of an after-hours service request at a County facility, designated Maintenance and Operations Team staff will make appropriate contacts to gain entry as documented in SOSP Volume VIII.

Exhibit E

Central servers and essential devices (e.g., routers and primary switches) shall be protected from the effect of electrical power outages and fluctuations by the installation of Uninterrupted Power Supplies (UPSs). Central facilities shall be adequately protected against fire damage.

Confidentiality

Each administrator, application, and user that can access any part of the CalSAWS system (e.g., server, website, database, etc.) must have permission to access that system. Permission is given on the basis of need-to-know. That is, there is a business need for that administrator, application, or user to have access to the information in order to accomplish an assigned job function. Additionally, CalSAWS contractors must sign the appropriate Non-Disclosure Agreements prior to obtaining any access to CalSAWS systems or their contents.

Administrators must ensure that sensitive CalSAWS data is protected by encryption and/or by file and folder permissions and/or access control lists (ACLs), which are sufficiently stringent for the data being protected. Sensitive data (e.g., passwords) that traverse a CalSAWS network or the Internet must be protected at all times by approved encryption mechanisms (e.g., SSL, VPN).

Data Classification

The CalSAWS project will create and maintain a Data Classification Standard that describes the different data types processed on CalSAWS systems, their sensitivity, and protection mechanisms, including requirements around auditing and logging, backup, archive, purge, transmission, etc.

Integrity

The integrity protections on a system ensure resources operate correctly and data in the system is accurate. Integrity controls include documented procedures, access controls, management reviews, and audit trails. Many of the security measures that are discussed in other sections of this policy (e.g., authentication, access control, auditing and logging, etc.) also play a role in maintaining integrity.

Integrity can be further segmented into three categories: system, data, and message integrity. Specific measures for each category are described below.

System Integrity

Hardware and software integrity checking mechanisms must be used to periodically validate the correct operation of CalSAWS systems. Use of some or all of the following mechanisms will meet this requirement:

- Simple checksums, cyclical redundancy checks or cryptographic checksums
- Intrusion detection tools
- Network filter programs and firewall systems
- Version control procedures
- Version control tools
- Program change controls (change detection tools).

Where the system supports it, validation should occur automatically.

Exhibit E

Data Integrity

Security mechanisms must be applied to CalSAWS systems to ensure data integrity. Such mechanisms will protect CalSAWS systems and data from malicious or unintentional alteration and provide a mechanism to verify that the data has not been modified. Use of some or all of the following mechanisms will meet this requirement:

- Encryption techniques used during data or program storage and/or transmission
- Data reconciliation controls (where the sensitivity of the data warrants such a mechanism)
- Security labels (tags) applied to sensitive files
- Simple checksums, cyclical redundancy checks or cryptographic checksums

Anti-Virus

An evaluated and approved anti-virus package will be installed and used on Windows servers, workstations, and laptops, to reduce operational risk associated with viruses or other malicious software. The software must be configured to scan files accessed in real-time as well as perform regular scheduled scans of files on the system. Email, including attachments, will be scanned at the email gateway or server before it reaches a user's mailbox. All outbound Internet email will be scanned before reaching the Internet.

Where supported by the system, anti-virus software will be configured to automatically retrieve new definitions on a regular basis. Anti-virus definitions that require testing prior to implementation will be tested and implemented as soon as possible. While a server is without anti-virus software, it must not be connected to the Internet or to the CalSAWS network.

Message Integrity

As of the writing of this policy, the encryption of email and system messages is not feasible in the CalSAWS environment. There is to be no expectation of the confidentiality or integrity for email or system messages that are not encrypted.

Denial of Service (DoS or DDoS)

Denial of Service (DoS) or Distributed Denial of Service (DDoS) is an attempt to prevent or interrupt authorized access to resources or the delaying of time-critical operations.

A denial of service is most commonly associated with an external entity or entities attempting to prevent access to resources by sending large amounts of traffic, usually mal-formed, in an attempt to use up available bandwidth or exhaust resources, thereby preventing normal access. A less common occurrence can be something internally sourced within the CalSAWS network attempting to do the same.

With regards to an Internet (or externally facing) attack, CalSAWS has decided to not take any action other than to absorb the extra traffic. The network team will identify as much as they can regarding the source of the traffic and then work with our Internet Telco provider to block the source from coming inbound. Information about the attack will be escalated to the CalSAWS Systems Security Officer.

With regards to an internal based attack (within the CalSAWS network), the network team will identify the source of the traffic and block it as close to the source as possible. Information about the attack will be escalated to the CalSAWS Systems Security Officer.

Exhibit E

Denial of Service (DoS or DDoS) Monitoring

Detection

The FireEye, BigIP F5's, Cisco ASA's and Splunk servers are systems within CalSAWS that will work together to help identify and mitigate Denial of Service (DoS or DDoS) attacks on targeted CalSAWS resources.

The centralized FireEye devices continually monitor incoming production network traffic. The device has the capability to monitor for known DDoS attacks (along with other malicious attack signatures). If an attack is identified by the device, then information about the attack is captured and logged. The device then sends out an immediate notification to the CalSAWS network team. Message will have subject line similar to: "DOS Attempt" or "DoS" (i.e. "Wonderware Suite Link DOS Attempt or Symantec DNS Response DoS"). The CalSAWS Network team will immediately investigate and provide confirmation of any real problems. Once a real problem has been identified, the team will follow the notification / escalation process to alert the appropriate support groups / CalSAWS security officer.

The BigIP devices and ASA devices (firewalls/vpn gateways) also have a default capability to detect and report on known DoS / DDoS attacks. The BigIP F5 will generate an alert with either the header "A DOS attack start was detected for…" and the ASA device will generate and alert with "ASA's = %ASA-4-733100: [DoS attack]". These messages are immediately forwarded to the central syslog server.

The Splunk server is configured to continuously monitor for specific pattern messages that have been pre-configured. Upon receiving a positive match, the Splunk tool immediately sends out a notification to the CalSAWS network team. The CalSAWS Network team will immediately investigate and provide confirmation of a real problem. Once a real problem has been identified, the team will follow the notification / escalation process to alert the appropriate support groups / CalSAWS security officer.

1.1.1.1 Alert and Escalation Notification

Upon identifying and capturing attack data, the network performs the appropriate procedures for escalating and alerting of the attack. Email, telephone, IM and the ticketing system is utilized depending on severity of the incident to notify and engage the appropriate support groups.

Apply Appropriate Mitigation Configuration

Review of the DDoS attack data will be performed by the appropriate support group. Based on attack type, changes to the appropriate system or network device will be requested and scheduled for implementation through the CalSAWS change management processes.

Availability

Security supersedes availability. If a system cannot be made available in a secure mode, the system must be made unavailable.

Auditing and Accountability

The following policies will be followed for auditing and accountability within the CalSAWS environments. The CalSAWS Maintenance and Operations Team is responsible for regularly reviewing audit logs to ensure that misuse of the system is caught and dealt with in a timely manner.

Exhibit E

Violation Escalation

The following is the escalation procedure for PII Security violations by county personnel:

1. First offense for a county each year:
   Inform Consortium, individual and Regional Manager
   Suggest Regional Manager informs individual's supervisor
2. Second offense for a county each year:
   Inform Consortium, individual and Regional Manager
   Regional Manager to report at Project Steering Committee
3. Third offense for a county each year:
   Inform Consortium, individual and Regional Manager
   CalSAWS Executive Director informs County Director

Legal Notice

User and administrator laptops and workstations, as well as network devices (routers, switches, etc.) and servers must be configured to display a legal notice prior to allowing access to resources. The legal notice must include the following five elements, at a minimum:

- The user is using a CalSAWS system
- CalSAWS systems are for authorized use only, in accordance with CalSAWS policies
- CalSAWS systems may be monitored for improper use
- Use of the system constitutes consent to monitoring
- Unauthorized use may result in reprimand, dismissal, financial penalties, and/or legal action.

The following Legal Notice phrasing has been approved for use with CalSAWS systems:

> This is a California Statewide Automated Welfare System ("SAWS") Consortium IV Joint Powers Authority ("CalSAWS") computer system, which may be accessed and used only by authorized users. Any and all unauthorized access or use of this computer system is strictly prohibited and violators may be subject to criminal, civil, and/or administrative action. Individuals using this system are subject to having all of their activities on this system monitored, intercepted, recorded, read, copied, and disclosed by and to CalSAWS management as well as law enforcement officials for official purposes, including without limitation criminal investigations. Anyone using this system expressly consents to such monitoring. By accessing or using this computer system, whether as an authorized or unauthorized user, it is assumed that you acknowledge the above statement and that you agree to these requirements.

The CalSAWS application must provide the above information via a Terms of Use or Legal Notice page or screen. These can be provided as links or mouse-over pop-ups from the home web page, the login page, or via the Help function in the application.

It is prohibited to manually or systematically disable the Legal Notice. Where possible, the system shall prevent users from disabling the legal notice on their machines.

Devices to be Audited

Devices that have logging capabilities, including operating systems, databases, applications, firewalls, routers, switches, etc., will be configured to produce a security audit log. Events and information will be logged as outlined in this Policy, and as detailed in the CalSAWS Auditing and Logging Standard.

Exhibit E

Events to be Logged

The CalSAWS logging components will collect and report on security relevant events sufficient to conduct an investigation. The following events must be recorded, at a minimum:

- Logons and logoffs
- Creation, modification or deletion of selected files (only those containing critical, highly sensitive CalSAWS data)
- Privileged actions taken by computer operators, system administrators, and/or system security administrators.

Information to be Logged

The CalSAWS logging components will collect and report on the following information, at a minimum, about recorded events in the security audit trail file(s):

- Date and time of the event
- The user ID on whose behalf the subject program generating the event was operating
- Type of event (e.g., create file, invoke displayed menu item, etc.)
- Success or failure of the event (e.g., failed user authentication attempts)
- Origin of the request (e.g., terminal ID) for identification and authentication events
- Name of object introduced, accessed, or deleted from a user's address space (e.g., file open, database table accessed, etc.).

To ensure proper recording of event times, CalSAWS will implement an approved and appropriately redundant Network Time Protocol (NTP) system, with which CalSAWS computers will synchronize their system clocks.

Automated vs. Manual Logging

Security-relevant events that meet security audit requirements (e.g., attempts to access unauthorized functionality) will be collected, processed, and stored by automated means whenever possible. Moreover, such automatically collected Security Audit Trail data will survive system restarts. Otherwise, manual logs will be used to supplement automated techniques (e.g., hardware maintenance actions cannot normally be audited by the system itself, but rather get recorded in daily maintenance logs).

Log Review

Logged information will be made available immediately after the information is recorded, so that the designated security auditors can responsibly fulfill their review obligations.

Protection of Audit Files

Access to security audit trail files and their recorded information will be limited to authorized people (e.g., stored audit trail files will be protected by the system from unauthorized changes or destruction). Printed audit records and audit records backed up to removable media will be placed in a secure area where only authorized personnel can access the media.

Exhibit E

Log File Maintenance and Retention

To provide availability of a complete audit trail, log capacity will be planned such that logs do not overwrite themselves in between backups. Furthermore, systems will be configured to gracefully shut down in the event that the audit log space becomes full.

Security log files will be stored in system-protected files. Log files must be available for a minimum period of one year. Security log files must be deleted once there is no longer a business or security need.

Vulnerability Assessment

As part of the auditing regimen, and to verify compliance with this policy and related standards, CalSAWS systems will have periodic vulnerability assessments executed via an evaluated and approved vulnerability assessment tool or suite. Such a vulnerability assessment tool or suite must be able to identify, describe, and provide a criticality ranking for potential system vulnerabilities, including, but not limited to, services/ports used, password weaknesses, inactive user accounts, missing security patches, and inadequate auditing configurations.

Vulnerabilities must be repaired in a timely manner, according to the value of the system and the risk that the vulnerability poses. Any vulnerabilities that cannot be repaired due to specific business needs, or if such repair interrupts required functionality in the system, will be thoroughly documented and approved by the Systems Security Officer. Otherwise, the system must be disconnected from the CalSAWS network until the vulnerability is removed.

Non-Repudiation

CalSAWS does not currently have or require a standard non-repudiation mechanism. Any future use of non-repudiation mechanisms must be reviewed and approved by the Systems Security Officer prior to implementation on any CalSAWS system.

Platform Security

CalSAWS systems, whether connected to the Internet or not, will be properly hardened. The only allowable exception is those systems that must be configured according to written County specifications, where such County specifications are in conflict with those provided by CalSAWS. Where County specifications do not exist, CalSAWS standards will apply.

CalSAWS will not operate platforms for which the vendor no longer provides security updates and patches. Security updates and patches will be tested and applied to applicable CalSAWS systems in a timely manner, according to the value of the system and the risk that the un-patched vulnerability poses.

Every machine on the CalSAWS network will have an identified owner (individual or organization), who will be responsible for providing the requisite security for that machine.

Network Security

CalSAWS will make use of firewalls, proxy servers, routers, switches, intrusion detection systems, and other similar devices to adequately protect the perimeter of each data center, as well as to monitor user and data traffic.

CalSAWS data centers will be protected by properly configured firewalls and intrusion detection systems.

Exhibit E

CalSAWS systems may be connected to the Internet, or via private connections to Counties, vendors, and other parties. Systems with external connections will be protected by hardening and firewalls. Externally facing systems will be placed in a Demilitarized Zone (DMZ) or other similar configuration to protect internal CalSAWS systems. Devices on the CalSAWS internal (trusted) network will not be accessible from the Internet unless the CalSAWS standard VPN solution is used. All external connections to CalSAWS networks must be registered with and approved by CalSAWS security personnel.

CalSAWS Remote Office Network Access Restrictions

The following network access restrictions apply to CalSAWS Remote Offices:

- Permit CalSAWS Remote Offices access to the CalSAWS Data Centers
- Permit Internet traffic from CalSAWS Offices, as appropriate
- Permit TCP and approved UDP sessions from CalSAWS Remote Offices to the County Network (see CalSAWS router ACLs for details)
- Permit ICMP from CalSAWS Offices for troubleshooting purposes to the County Network
- Deny inter-office traffic over the CalSAWS Network (except for approved applications – see CalSAWS router ACLs for details).

County Office Network Access Restrictions

The following network access restrictions apply to County Offices:

- Permit ICMP from County Network to CalSAWS Offices for troubleshooting purposes
- Restrict UDP and deny TCP sessions from County Offices to CalSAWS Remote Offices (see CalSAWS router ACLs for details)
- Restrict traffic from County Offices to CalSAWS Data Centers (see CalSAWS firewall ACLs for details)
- Permit Internet traffic from County Offices to CalSAWS Internet sites.

Inter-Data Center Network Restrictions

The following network access restrictions apply to network traffic that moves between County/Departmental Data Centers and CalSAWS Data Centers:

- Permit FTP traffic between the County/ Departmental Data Center and CalSAWS Data Centers' Extranet DMZ over the CalSAWS Extranet WAN
- Permit encrypted FTP traffic between the County/ Departmental Data Center and the CalSAWS Data Centers' Internet DMZ over the Internet
- Permit traffic required for NT Trusts between the County/ Departmental Data Centers and the CalSAWS Data Centers over the CalSAWS Network. This is restricted by port and source hosts and destination hosts.

Remote Access

All remote access to the CalSAWS network must be through one of the approved channels (Nortel VPN in conjunction with dial-up or equivalent).

Sensitive CalSAWS data accessed from off-network locations must be transmitted over an encrypted channel such as virtual private network (VPN) or secure sockets layer (SSL). Access to administrative functions from outside the CalSAWS network, without the use of VPN, is prohibited.

Exhibit E

Inbound dial access to any device connected to the CalSAWS network, with the exception of approved remote access services and temporary access for vendor troubleshooting or repair, is strictly prohibited.

System administration via remote connection is permissible only via secure channels (e.g., VPN, SSH, or similar).

Configuration of Network Infrastructure Devices

Network infrastructure devices, including routers, switches, firewalls, etc., will be adequately hardened to prevent unauthorized access, in accordance with applicable CalSAWS standards. Configuration of the permissions for these devices will follow the Lease Privilege Principle.

Wireless Networks

Wireless networks are inherently insecure. Prior to implementing any wireless system within CalSAWS, the implementation team must obtain approval from the Systems Security Officer.

Application Development

CalSAWS application releases must be developed, deployed, and maintained securely, in accordance with regulations in this policy. Security requirements (such as identification, authentication, access control, confidentiality, integrity, non-repudiation, availability, and accountability mechanisms) will be revisited at the inception of each new release cycle. Each release will meet security requirements as appropriate for the data that will be handled, and the users that will have access to the application.

To ensure security compatibility, new releases will be developed on production-like hardened systems, and developers will use permissions similar to those that the application users will have. Existing releases must be remediated if they cannot function on systems that have been hardened in accordance with this policy.

Application releases must be tested for security before being put into production. However, production data must not be used in the development or test environments without the explicit permission of the data owner.

Secure Operations

Software Updates and New Releases

New systems and significant configuration changes (e.g., major releases, addition of new features) that may adversely impact the security of CalSAWS systems must be reviewed and approved by the Systems Security Officer.

Disaster Recovery and Business Continuity

CalSAWS will have documented Disaster Recovery and Business Continuity plans, which adequately interact with and complement existing County plans. The Disaster Recovery and Business Continuity plans will include roles and responsibilities, contact information, communication requirements, reaction and repair timeframes, requirements for hot, warm, or cold backup sites, migration plan for moving to a backup site or restoring operations at the original site, and so on. Disaster Recovery and Business Continuity plans will be periodically tested and reviewed for accuracy and completeness.

Exhibit E

Backups and Security of Backup Media

In support of the CalSAWS Disaster Recovery and Business Continuity plans, and to prevent data loss and work interruption, CalSAWS data, as well as software and firmware configurations, will be backed up regularly. Backup frequency must be commensurate with the criticality and volume of information on any given system.

Backup media, whether stored at CalSAWS or an off-site location, must be physically secured to prevent unauthorized access or damage from heat, humidity, and other environmental hazards.

Prior to disposing of storage media such as tapes, hard drives, disks, etc., or sending to the vendor for servicing, sensitive data must be completely removed so that it is no longer retrievable.

Examples and Frequently Asked Questions

The following examples and/or frequently asked questions have been provided to help illustrate the implementation of this Policy.

Q: What does ’appropriate’ mean?

A: This policy provides general guidance, and in some cases cannot specify what is appropriate. The owner of a system or a set of data must decide what appropriate means for his or her system or data based on use, sensitivity, value, etc.

Q: What qualifies as a security event?

A: A security event is any event – whether intentional or accidental – that adversely affects the confidentiality, integrity, or availability of CalSAWS data or systems. There are many examples of security events. Some of the more common include intentional or accidental deletion or corruption of CalSAWS data, tables, or software.

Q: What does ’periodically’ mean, and why are timeframes not better specified in the policy?

A: One of the key definitions of a policy is that it requires little modification over time. Therefore, words like ‘appropriate’ and ‘periodically’ are used. Periodically should be taken to mean as often as reasonable to maintain a good security posture, without overly burdening the business. In many cases, other CalSAWS documentation such as the SOSP provides more concrete timeframes for statements in the policy.

Q: What are appropriate ways to protect administrator passwords?

A: It is important for the security of CalSAWS systems that administrative accounts on each server have different passwords. As such, it is possible for administrators to have to keep track of literally dozens of passwords, and given their complexity, it may not be reasonable for an individual to remember so many. That is why the provision was made that administrators can write down a portion of each password, as a memory aide. It is important that administrators not write down the entire password, as that facilitates compromise. Passwords should never be stored on an electronic system or in a centralized repository for the purposes of retrieval, because it is too difficult to ensure that the system or repository cannot be compromised. Also, it is difficult to ascertain if passwords have been viewed on an electronic system. Passwords that are stored on electronic systems for the purposes of authentication must always be stored in one-way encrypted format. Administrator password fragments that are written down should be stored on a piece of paper that is sealed in an envelope and locked in a secure location, such as a cabinet, drawer, or safe. If the envelope is opened or lost, all passwords written

Exhibit E

therein must be immediately changed, and the incident reported to the CalSAWS Systems Security Officer.

Exhibit E

2 Appendix A

Information Security Glossary

This section provides a definition of the terms and acronyms used in the CalSAWS Information Security Policy.

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Term	Definition
Access Control	The process of limiting access to the resources of an IT system so that only authorized users, programs, processes, systems or other IT products may have access.
Access Role	An access role is the specific access granted to a user across all systems based on the user's job function. Each job function has a corresponding access role.
Accountability	The ability to assign personal responsibility for using a system or its capabilities to a specific person or groups of persons.
Administrator ID	The unique login ID for an individual that requires administrative privileges on a system.
Anti-Virus	Software that attempts to detect and clean virus or virus-like software on servers or workstations. It is often implemented using anti-virus definitions (see below) as well as heuristic algorithms.
Anti-Virus Definition	A file containing “signature” pieces of virus code. Various types of network traffic are searched for virus signatures in the definition. If any signatures are detected, the anti-virus software alerts the user that they have a virus on their machine, and assists the user in removing the virus.
Application ID	The unique login ID assigned to an application that it uses to access various resources. At the operating system level, an application might access file system resources. At the database level, an application might use its ID to run queries. Application IDs should only be used by the applications to which they are assigned, not by human beings.
Assurance	Confidence that the security strategy for a system, and its countermeasures and safeguards, will accurately and properly mediate and enforce the security policy.
Audit Trail	A chronological record of system activities that is sufficient to enable the reconstruction, review, and examination of an event sequence leading to or following a particular result. Formally, it is called the Security Audit Trail.
Auditing	The process and/or capability of gathering information on transactions and system administration functions to validate authorized system use, and to discover potential unauthorized system use.
Authentication	The process of identifying and ensuring that an entity is who it claims to be. For individuals this is usually based on entering the correct password associated with a login ID. Authentication merely ensures that the individual is who he or she claims to be but says nothing about the access rights of the individual.
Authorization	The process of validating that someone has the rights to access something.
Availability	The operational aspects of the security solutions that assure that the system is consistently accessible to users when they require access.

Exhibit E

Term	Definition
Back Door	A segment of programming that a hacker or developer leaves behind on a system in order to be able to get back in at a later time.
Biometrics	An authentication process in which an individual's identity is validated through unique physical characteristics such as fingerprints, iris/retina/voice patterns, facial/hand contour, etc., instead of a password.
Brute Force	A classic attack technique whereby all possible combinations are attempted until one succeeds. This typically refers to cryptography, either finding the right key to decrypt a message, or discovering someone's password.
Choke Point	The concept that security should be performed at a small number of points. Processes, networks, applications, etc. should be funneled through a choke point to ensure that the security checks occur.
Computer Security	The protection resulting from all measures designed to prevent deliberate or inadvertent unauthorized disclosure, acquisition, manipulation, modification, or loss of information contained in a computer system, as well as measures designed to prevent unauthorized system use.
Confidentiality	Confidentiality refers to the degree to which data is protected from interception by a third party when sent over the network. A high degree of confidentiality indicates that the sender and receiver of a particular set of data are the only ones able to view that data. Confidentiality over the network is ensured by correctly implementing an encryption mechanism.
Content Inspection	A method to detect and remove or block any harmful or inappropriate content before it can cause damage or be accessed.
Cookie	A block of ASCII text that a web server can pass into a user's Web browser to track a client through multiple HTTP requests. The advantage is that a cookie can automatically identify the client to the server, thereby improving the usability for the user, by providing identification and customization capabilities. The downside is that cookies are often placed on the client computer without the knowledge of the user, giving rise to concerns about privacy through electronic trespass, and creating the potential for impersonation.
Cryptography	A mathematical model that allows for the “scrambling” of data in a way that is irreversible without having the right information. Cryptography protects the privacy of a transaction, assures contents of the transaction cannot be altered without detection, and provides non-repudiation with digital signatures.
Data Security	The protection of data from unauthorized modification, destruction or disclosure. Unauthorized in this case can mean either accidental or intentional.
DBA	Database Administrator
Denial of Service	The prevention of authorized access to resources or the delaying of time-critical operations.
Dictionary Attack	A dictionary attack is an automated process that can compare words in a dictionary against a password in an attempt to "crack" it. Such a process can also combine words, change capitalization, and append numbers.
Digital Certificate	An electronic certificate issued to each user containing cryptographic information. The user uses their certificate to digitally sign and/or encrypt data.
Digital Notarization	The process of ensuring that electronic information, such as a document or file, contained specific content at a specific moment in time and can be proven to not have been modified since then.

Exhibit E

Term	Definition
Digital Watermark	A method of copy protection for web data that involves making very small, hidden alterations to the data to store a form of identification of the material. Images, sound files, and data can be examined with programs that find and display the identifying information, showing the true owner and possibly the name of the person for whom the copy was first produced.
Encryption	The process of making information unreadable to protect it from unauthorized viewing or use, especially during transmission or storage. Encryption is based on a cryptographic algorithm and at least one key. Even if the algorithm is known, the information cannot be decrypted without the key(s).
Fail-safe	A fail-safe device is configured to revert to a more secure mode of operation when in an error state (e.g., by shutting down).
Firewall	A system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially intranets. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.
Harden/Hardening	The word "harden" implies putting a shell around a computer in order to protect it from intruders. Typically, hardening means removing or disabling unneeded or insecure services; applying patches to fix known vulnerabilities; and removing default accounts and services.
Hash	A cryptographic operation where an entire message is run through some mathematical operations resulting in a fixed-length (e.g. 128-bit) string that is probably unique. This "hash" has two important properties: It is "one-way"; given a hash, somebody cannot figure out what input message generated the output hash. It is unique. No two messages will produce the same hash.
Hazard	The ability of a threat to use a vulnerability to cause harm. This includes the presence of the threat, the motive of the threat to cause harm, and the vulnerability that allows them to cause harm.
ID	Identification
Identification	Identification is the process that enables recognition of an entity by a system through any of several means. This is typically achieved via a login ID, employee ID, etc.
IDS	Intrusion Detection System
Integrity	Integrity is a measure of the accuracy of data storage and transmission. Storage of data, or transmission of data through a system with low data integrity will result in data corruption or loss. Data integrity can be validated in a number of ways, including checksum methods and data packet checking.
Intrusion Detection System	A system that can detect suspicious activities on a network (network IDS) or on a platform (host-based IDS). It works by recognizing common patterns through statistical profiles or rule-based systems that may indicate an attack. Intrusion detection tools provide a fast and automated mechanism that allows a company to be more pro-active in identifying and stopping intruders. Intrusion detection.
LAN	Local Area Network

Exhibit E

Term	Definition
Least Privilege Principle	A fundamental rule from trusted system theory that requires each subject be granted the most restrictive set of privileges needed for the performance of authorized tasks. Application of this principle limits the damage that can result from accidental, erroneous, or unauthorized use of a corporate system.
Log Scanners	These tools will recognize system activity patterns and generate reports or alarms if suspicious activities occur.
Logging	The primary method to trace problems and security breaches in a network or IT system. By logging events from multiple devices an operator can trace the events leading up to a problem and determine the cause of the problem. Logs can be used for reactive actions as well as preventative actions.
Login ID	Generic term for the name by which a user or application is identified to the system. User IDs, application IDs and administrator IDs are different types of login IDs.
Login	Procedure used to establish the identity of the user and the levels of authorization and access permitted.
Logout	Procedure used to terminate computing sessions.
MAC Address	Media Access Control Address. A hardware address that uniquely identifies each node of a network.
Non-Repudiation	Method by which the participants in an electronic transaction are provided with proof of the transaction, so that neither can later deny having participated the transaction. Examples of an electronic transaction include the sending/receipt of an email, the signing of a digital contract, or the transmission/receipt of a purchase order.
NOS Password	Password used to access the CalSAWS Workstation and CalSAWS Network
Pass-through Authentication	In Windows domains containing Windows NT servers, if security is not properly configured, a user having the same user-ID and password combination in two domains can jump from servers in one domain onto servers in another domain without re-authenticating. This can lead to incomplete audit trails or the user gaining unauthorized access.
Passcode	A passcode is the combination of a user’s Personal Identification Number (PIN) and the six-digit code that is displayed on the user’s SecurID token. The passcode changes every 60 seconds as the token code changes.
Password	A password is a secret string of characters that a user must know in order to gain access to a system. The password is entered in conjunction with a login ID for the system to validate. A passphrase is a correspondingly larger secret consisting of multiple words or strings.
Password Strength	Password strength is a measure of how difficult (or easy) it would be to guess or “crack” a password.
Patch (Fix, Update)	Security updates to products are often referred to as “patches” because they fix one small part of the product rather than updating the entire product.
Personal Identification Number	A personal identification number is a user-selected string of four to eight digits that is used in conjunction with a SecurID token code to authenticate to a system.
PIN	Personal Identification Number.
Platform Security	A method of securing the platform on which sensitive servers and applications run. A failure to secure the platform may result in the platform, server and application being compromised.
PRT	Policy Review and Training environment

Exhibit E

Term	Definition
Public Key Cryptography	A type of cryptography that uses a key pair of mathematically related cryptographic keys. The public key can be made available to anyone who wishes to use it and can encrypt information or verify a digital signature; the private key is kept secret by its holder and can decrypt information or generate a digital signature.
Public Key Infrastructure (PKI)	The architecture, organization, techniques, practices, and procedures that collectively support the implementation and operation of a certificate-based public key cryptographic system.
RCA	Remote Console Access
Registration	The process of creating new users in a system. Ensuring proper registration of users is necessary to allow effective ongoing authentication.
Remote Console Access	Full control (shell or GUI) access to a system where the communication between the input and display devices (e.g., keyboard and monitor) and the system being accessed travel over a shared data network.
Risk	The probability that a particular threat will exploit a particular vulnerability of the system. Risk is more conveniently defined by an equation: *Risk = Likelihood of Threat Occurring x Loss Incurred*
Risk Analysis	An analysis of system assets and vulnerabilities to establish an expected loss from certain events based on estimated probabilities that those events occur. A risk analysis helps determine whether countermeasures are adequate to reduce the probability of loss, or actual loss impacts, to an acceptable level.
Risk Audit and Assessment	Processes that identify vulnerabilities and potential threats to determine what risks are of concern to the organization and what degree of risk is acceptable to the organization.
Role-Based Access Control (RBAC)	With RBAC, security is managed at a level that corresponds closely to an organization’s structure. Each user is assigned one or more roles, and each role is assigned one or more privileges that are acceptable for users in that particular role. Roles can be hierarchical. Role-Based Access is always assigned using the Least Privilege Principle.
Security Administration	Managing all IT users within an organization. The difference between security administration and security operations is that security administration performs user management functions whereas security operations supervises those and other functions.
Security Architecture	The components, such as tools, processes, policies and standards, that together enables a secure IT architecture to be deployed and operated. A security architecture may be part of a development, execution or operations architecture.
Security Awareness	A top-down plan that sets an organization’s expectations regarding information security, explaining each individual’s responsibility for protecting the confidentiality, integrity and availability of the organization’s business assets.
Security Compliance	The functions that people in an organization perform to ensure that security policies and procedures are created, followed, measured, enforced, and updated as required.
Security Development	The review, definition, design, and implementation of security solutions. Security development supports and enables the building of new security technologies, architectures, applications, systems, and business capabilities, as well as new security services and security infrastructure.

Exhibit E

Term	Definition
Security Infrastructure	Security components including methodology, services, and tools, which provide protection for an organization's business assets.
Security Incident	An intended or unintended breach in security, usually resulting in unauthorized access to information or a system.
Security Incident Response	The process of responding to a security breach, including stopping the breach if in progress, preventing its reoccurrence, and investigating the circumstances of the breach
Security Investigation	If there is suspicion or confirmed evidence of a security breach, it is critical that an investigation is performed quickly. An incident response team will assess the immediate risk to the business assets as a result of the incident and take appropriate short-term actions.
Security Management	Processes that initiate and manage enterprise-wide security programs to support the corporation's business goals, thereby developing, building and maintaining the security organization and shape its structure.
Security Auditing or Monitoring	The tracking of relevant security events and the subsequent actions to be taken when such events occur. Security Auditing or Monitoring is performed through a combination of security tools and manual checks.
Security Operations	The ongoing monitoring of security components and security events within an organization. Security monitoring refers to the tracking of relevant events and the subsequent actions to be taken when such events occur. The difference between security operations and security administration is that Security Operations supervises security administration and other functions whereas security administration performs user management functions only.
Security Policies, Procedures, Standards and Guidelines (PPS&G)	Guiding principles that form the foundation for all security related activities of an organization, aiming to achieve consistency in architecture and to reduce the risk, effect and cost of security incidents.
Security Strategy	Processes that set the future directions for information security within an organization and determines the overall plan for the security based on new threats, user requirements, development requirements or vendor strategies.
Security Tools	Tools that support security management services and the people performing the security functions and processes.
SET	Secure Electronic Transaction is an open specification for sending encrypted credit card numbers over the Web.
Single Sign-On	A process that enables a user to sign on using a single UserID and be connected to multiple systems without having to sign on to each one of them. Single sign-on provides two main benefits: a user-friendly system and a system that is easy to administer.
SSID	Service Set Identification. An identifying number that is statically configured on both the wireless access point and client machines.
SSL	Secure Sockets Layer is a transport level technology for authentication and data encryption between a Web server and a Web browser.
Strong Authentication	Verifying a user's identity by using at least 2 of the 3 available factors: something you know (e.g., password), something you have (e.g., token), something you are (e.g., biometrics).
System	A system can be an operating system, an application, a database, a stand-alone server, a Windows domain, or similar.
Threat	Any circumstance or event with the potential to cause harm to a system in the form of destruction, disclosure, modification of data, and/or denial of service. Threats can be human or environmental, malicious or accidental.

Exhibit E

Term	Definition
Token	A physical device that is used in some authentication schemes to verify the identity of a user. Without physical possession of the token the user cannot prove their identity.
Trojan Horse	A program that resembles a program that a user wishes to run (such as a game, a spreadsheet, or an editor). While the program appears to be doing what the user wants, it actually is doing something else unrelated to its advertised purpose, and without the user's knowledge.
User ID	The unique login ID for an individual that does not require administrative privileges on a system.
Virus	A sequence of code that is inserted into other executable code, so that when the regular program is run, the viral code is also executed.
Virtual private network (VPN)	A secure WAN, also known as an encrypted tunnel, built atop a public network, such as the Internet. Hosts within the VPN use encryption to talk to other hosts. The encryption excludes hosts from outside the VPN even if they are on the same public network.
Vulnerability	A weakness in system security procedures, system design, implementation, internal controls, etc., that could be exploited to cause harm.
Vulnerability Assessment Tools	Tools that assist in finding common security holes and help to eliminate them by hardening the systems on which the holes were found. Vulnerability assessments are generally performed on all hosts and servers, critical or non-critical. Often these tools measure against a set of criteria or standards. Vulnerability assessment tools assist in closing the gap between the security policy and actual security by providing information about security vulnerabilities.
WAN	Wide Area Network
WEP	Wired Equivalent Privacy. A security protocol for wireless networks that is defined in the 802.11b standard. WEP has been highly exploited and is no longer considered secure.
Worm	A program that can run independently and travel from machine to machine across network connections.

Exhibit E

CalSAWS User Security and Acceptable Use Policy

Overview

CalSAWS assets and information within the project's control and use must be used in a secure, approved, ethical, and lawful manner and in accordance with the terms and conditions of the CalSAWS contracts to appropriately protect such assets and information. This policy applies to all systems operated by the CalSAWS Joint Powers Authority (JPA) including the legacy C-IV, legacy CalWIN and LRS systems (hereafter collectively referred to as "CalSAWS Systems").

Purpose

The purpose of this Security and Acceptable Use Policy ("Policy") is to outline appropriate user security and acceptable use requirements relating to the CalSAWS assets and information that are within the project's control and use.

Scope

This Policy applies to all CalSAWS Project personnel across all organizations, as well as all outside vendors who are provided with access to CalSAWS Systems as part of the contract work such vendors are providing to CalSAWS (hereafter collectively referred to as "Personnel").

Compliance

Security and acceptable use, as described herein, are the responsibility of all Personnel. Non-compliance with the required measures and behaviors outlined in this Policy could pose significant business and legal risk to the CalSAWS Consortium, organizations in the Consortium, and/or the offending Personnel, and could negatively impact CalSAWS operations. Therefore, your full understanding and compliance with this Policy is mandatory. Failure to comply will be reported and appropriate action taken, which may include, but is not limited to, financial penalties, termination of employment, legal action, or other steps as appropriate. Applicable county discipline procedures will be followed for Consortium personnel. If you become aware of any breach or potential breach of this Policy by you, outsiders, or any Personnel, immediately contact your supervisor.

Precedence

Personnel must follow this Policy in addition to the acceptable use and security policies of their organization. In the event of a conflict between this Policy and their organization's policies, Personnel will adhere to the more stringent policy. Personnel will clarify policy conflict questions with their supervisor or CalSAWS Technical Support. Supervisors that do not know the right course of action must consult CalSAWS Security Officer.

Exhibit E

General Provisions

CalSAWS systems, including but not limited to computer equipment, software, operating systems, storage media, network access/accounts providing electronic mail, web browsing, FTP, and any data that is the property of CalSAWS must be used in a secure manner, and may only be used for authorized CalSAWS business purposes relating to the CalSAWS Project.

There is one general requirement with respect to use of CalSAWS systems:

- Personnel must not take any actions that could cause harm to CalSAWS systems, resources, assets, facilities, or Personnel.

Security Requirements

Password Responsibilities

The disclosure of Personnel passwords is strictly prohibited. Personnel are responsible for maintaining the secrecy of their passwords and will be responsible for any misuse of their accounts as a result of inappropriately disclosed passwords. No Personnel are authorized to request the password of other personnel, including Technical Support staff.

Passwords to CalSAWS systems must be created and maintained in conformance with this Policy and the CalSAWS Information Security Policy.

Personnel are responsible for upholding password policies, even if the system does not or cannot require that all requirements be met.

Sensitive Information

Personnel shall not provide non-public CalSAWS Project-related information, such as names of Personnel, contact information, user IDs, or project details (“Sensitive Information”) to any unauthorized destinations, without first confirming with their supervisor whether the release of such Sensitive Information is acceptable. Sensitive Information that is in electronic format must be protected by enabling password protection, stringent file permissions, or using an approved encryption mechanism. For details on acceptable encryption, please contact CalSAWS Technical Support.

Sensitive Information that is in printed format must be placed in a locked drawer or locked cabinet when not in use. When printing Sensitive Information, documents must be immediately removed from the printer.

Prior to leaving their work area, Personnel must log off from, or electronically lock their computers (including PCs, laptops, servers, and workstations). All computers connected to the CalSAWS network under Personnel control and use must be configured to automatically enable a password-protected screensaver after no more than 10 minutes of inactivity.

Special care must be exercised when removing Sensitive Information from the facility. Personnel must ensure that such information is protected in a comparable or superior manner to how it is protected in a CalSAWS facility. Sensitive Information may not be removed from a CalSAWS facility unless approved by CalSAWS Project Management.

Exhibit E

Any Personal Digital Assistant (PDA) device containing Sensitive Information must be configured to require password authentication prior to granting access. Where available, appropriate encryption mechanisms will be used.

Sensitive Information must be labeled as such, whether in electronic or printed form. Refer to the CalSAWS Data Classification Standard for additional details on classifying and protecting sensitive information.

Note: Sensitive Information should not be confused with confidential information. Confidential information consists of any oral, written or electronic information that either belongs to, has been developed by, or has been received from our client, CalSAWS, and has commercial value in their business, or the business of their affiliates, vendors, customers or clients and is not generally available to the public. Every Consortium employee, Contractor employee and subcontractor that rolls onto the CalSAWS engagement is required to review and formally acknowledge this policy.

Personal Information

Personnel shall comply with the provisions of Section 10850 and 18909 of the Welfare and Institutions Code, Division 19 of the California Department of Social Services Manual of Policies and Procedures, and all other statutory laws relating to privacy and confidentiality. The referenced Welfare and Institutions codes stipulate that the data is confidential and shall not be disclosed.

In order understand the definition of data, the California Civil Code applies. As defined in California Civil Code section 1798.82, “any person or business that conducts business in California, and that owns or licenses computerized data that includes **personal information**, shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.” (e) For purposes of this section, "personal information" means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:

- Social security number.
- Case Number
- Driver's license number or California Identification Card number.
- Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

(f) For purposes of this section, "personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

Exhibit E

Personal Information may not be printed, faxed, emailed, or stored on a laptop. Personal Information may not be taken from the Application Development Facility. Exceptions to this must be authorized by Project Executive Management.

Email Responsibilities

Some Personnel may retain email accounts provided by their employer's (vendor or county). Such accounts are important for conducting confidential business and personnel matters. The Consortium manages and administers the CalSAWS.org email accounts to conduct project business.

Personnel shall utilize their CalSAWS email accounts to conduct CalSAWS-related business. Exceptions to the use of the CalSAWS email domain include the following:

- Non-Project communications
- Confidential personnel matters

Personnel must be aware that written communications may be subject to public disclosure pursuant to federal and state law, specifically the Freedom of Information Act (FOIA) and the California Public Records Act (CPRA). The CPRA was enacted in 1968 and codified as California Government Code § 6250 through § 6276.48. The fundamental precept of the CPRA is that government records shall be disclosed to the public, upon request, unless legally exempt from such disclosure or the public interest in nondisclosure clearly outweighs the public interest in disclosure. Some exemptions to public disclosure include:

- Preliminary drafts, notes, or memoranda that are not retained by the public agency in the ordinary course of business
- Personnel, medical records, or similar files, the disclosure of which would constitute an unwarranted invasion of personal privacy
- Applications or records concerning any individual in connection with any form of public social services under the California Welfare & Institutions Code §10850
- Deliberative processes, discussions, or negotiations
- Trade secrets or proprietary information
- Attorney-client privileged communications
- Records pertaining to pending litigation to which the agency is a party, or to claims, until the litigation or claim has been finally adjudicated or otherwise settled

Personnel must use caution when opening email attachments received from unknown senders, as they may contain viruses, worms, or Trojan horse code. Personnel should also be cautious of email from known individuals if the email subject or contents seem out of character for that individual. In such a case, Personnel should contact the sender and verify the validity of the email before opening it whenever possible.

Personnel must never reply to spam or take actions as requested in the message, such as clicking on a link, doing what it says about a virus, replying, or asking to be removed

Exhibit E

from the mailing list. “Unsubscribing” from unsolicited spam messages typically serves to alert the sender that a valid email address exists and will generally result in even more spam being sent. Spam messages should be disregarded and promptly deleted. Personnel should also notify technical support if the spam becomes a nuisance. Personnel must immediately open and act on any security message sent by CalSAWS Technical Support. Failure to do so can result in system compromise or data disclosure.

Unless it is received from CalSAWS Technical Support, Personnel must never take any action regarding virus notifications. Furthermore, Personnel must always let CalSAWS Technical Support handle communication to the project, remediation, and prevention. Personnel are advised that many publicly distributed emails containing virus warnings are hoaxes and following such emails can result in computer damage.

Instant Messenger Responsibilities

Instant messaging services typically do not provide encryption services and are thus not secure. Without encryption, instant messenger conversations are vulnerable to interception by unauthorized third parties. Personnel must never discuss Sensitive Information or transmit files containing Sensitive Information over unencrypted instant messaging services.

Instant messaging services make the CalSAWS network susceptible to viruses, as they provide an unprotected gateway from the Internet into the CalSAWS network. Personnel should only use instant messaging file transfer as a last resort, if email is unavailable. Any files received via instant messenger file transfer must be scanned with a virus scanner prior to being opened or executed.

A common mechanism for propagating instant messenger viruses is via URL links. Personnel should never click on a URL link sent via instant messenger if it appears unfamiliar or out of character for the sender. Personnel should contact the sender of any link that appears suspicious and ask about the validity of the link before attempting to access the site.

Other Security Responsibilities

Personnel are responsible for the following to help maintain CalSAWS system security:

- Personnel are prohibited from conducting unauthorized port or vulnerability scans or executing any form of unauthorized network monitoring.
- Personnel must not tamper with or circumvent user authentication or security of any host, network, or account.
- Personnel must maintain virus scanning utilities, personal firewalls, or other programs designed to protect systems, users, or information in good working order, with approved configurations intact.
- Personnel may not disable or modify any legal notice or warning banners on CalSAWS systems.
- Personnel may not tamper with or circumvent installed physical facility security measures.
- Personnel must safeguard Sensitive Information about security designs or implementations to prevent access by unauthorized persons.

Exhibit E

- Personnel must not set up or assist in the configuration of unauthorized network or telephone access points (e.g., modems or wireless access points).

Privacy and Monitoring

The workstations, laptops, and user accounts assigned to Personnel are provided to enable them to perform their jobs in the most efficient and effective way possible. However, Personnel are not entitled to any expectation of privacy in the materials or information that is created, sent, or received by them on CalSAWS systems. To the extent permitted by local, state and federal laws, the CalSAWS contracts, authorized Personnel (such as the CalSAWS Systems Security Officer, members of the Security Team, CalSAWS Technical Support, CalSAWS Project staff, CalSAWS authorized representatives, etc.) may examine any materials and information stored on CalSAWS systems without prior notice, as they feel appropriate. Some examples of situations may include investigation for a suspected breach of security, for the prevention or detection of crime, and other legally permissible situations.

Subject to local, state and federal laws, the CalSAWS contracts, CalSAWS may monitor any and all aspects of its computerized resources used by Personnel, including, but not limited to, monitoring sites visited by users on the Internet, monitoring chat groups and newsgroups, reviewing material downloaded from or uploaded to the Internet by Personnel, and reviewing email sent and received by Personnel. Wherever possible, monitoring will be carried out by methods which prevent misuse, such as automated monitoring software. Personnel must understand that CalSAWS may use automated monitoring software to monitor material created, stored, sent, or received on the CalSAWS network to ensure that inappropriate material is not created on, or transmitted via CalSAWS systems, and that inappropriate use of CalSAWS systems does not occur.

Incident Handling

Personnel must promptly report any suspicion of, or occurrence of, unauthorized activities as outlined in the CalSAWS Vendor Breach Notification Process. This includes suspected password compromise and inappropriate data disclosure. In the case of virus infection, or phishing suspicion, personnel should immediately contact CalSAWS Technical Support. Personnel should not take any action on their computers; as such actions could adversely affect a security investigation or the ability to safely eradicate malicious code.

Physical Security

During the day, Personnel must physically lock down their laptops with an approved cable lock device.

Personnel must safeguard any mobile devices and removable storage media containing CalSAWS information by concealing them in locked drawers or locked cabinets when left unattended.

With regard to physical access to the Project Management Office (PMO) or the CalSAWS project sites (Norwalk, Rancho Cordova and Roseville, Ca), Personnel must adhere the following:

Exhibit E

- All CalSAWS Project staff must visibly wear their Project ID badge each day while on site. If any CalSAWS Project staff has lost their badge, they must notify the Project Management Office (PMO) immediately so the lost badge can be deactivated, and a new one can be issued.
- All visitors (anyone who is not staffed on the Project and does not have a CalSAWS Project ID badge) must sign in at the front desk upon entry and sign out before exiting the CalSAWS Facility.
    - Visitors will be provided with a CalSAWS Visitor badge that they should visibly wear while onsite; this badge will be an inactive badge that will not open doors that have a proximity access pad. If necessary, a temporary proximity access badge can be checked out from PMO. Otherwise, these visitors should be escorted by the CalSAWS staff with whom they are meeting.
    - For onsite workgroups or other large onsite meetings:
        - The meeting coordinator should obtain a list of attendees from the County (or other appropriate organization) and provide that list to the CalSAWS Receptionist in advance of the meeting to help expedite the sign-in process.
        - A temporary proximity access badge that allows access to locked doors with a proximity access pad can be issued to the meeting/ workgroup coordinator and shared among the visitors. Large onsite meetings at the project site should be scheduled in Sutter Conference Room in Suite 150 when possible so that visitors can leave and re-enter the site without a proximity access badge.
        - All visitors must sign out at the front desk and return any CalSAWS Visitor badges and temporary proximity access badges before leaving the site.
- When the facility doors are locked, Personnel must not allow anyone access to the facilities unless the individual can be positively identified as authorized to access the facilities after hours. Personnel should not put themselves in physical danger to obey this Policy (e.g., protecting the facility's physical security does not include wrestling a gun from an intruder), however, they should immediately notify their supervisor if they feel that complying with this Policy would put them in such danger. Any suspicious persons noticed during non-business hours should be reported to the on-site security guard.

Acceptable Use Requirements

CalSAWS assets and information are to be used for authorized business purposes relating to the CalSAWS Project only.

Under no circumstances may Personnel engage in any activity that is illegal under local, state, or federal law while utilizing CalSAWS assets and information.

Personal Rights, Harassment, and Workplace Hostility

The following activities are strictly prohibited:

- Violating the rights of any person or company.

Exhibit E

- Using CalSAWS assets to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws.
- Harassing anyone via email, telephone, paging, or any other means of communication, whether through language, frequency, or size of messages.
- Browsing websites containing, storing, or displaying information or materials that are explicit, pornographic, or hate-based.

Infringement

Infringement of the intellectual property rights of others is a serious offense that could result in the prosecution of not only the individual perpetrator, but also of CalSAWS if the offense was carried out using CalSAWS assets and information. As such, the following are strictly prohibited:

- Violating information protected by copyright, trade secret, patent, trademark, or other intellectual property rights, or similar laws or regulations, including, but not limited to, the installation, storage, or distribution of "pirated" or other software products that are not appropriately licensed for use by CalSAWS.
- By definition, anything posted on the Internet that is an original work (including email, pictures, jokes, artwork, music, etc.) is protected by copyright law(s), whether or not it is explicitly indicated that the work is copyrighted, or the copyright (©) symbol is included. Therefore, Personnel may not use such original works of authorship (e.g., by using “cut and paste” or “copy and paste”) or download music or videos without the author’s (or artist’s) express permission. In a text-based document, merely changing a few words or “scrubbing” (i.e., removing) the specific references to names or other identifiers in the document is not enough to avoid copyright infringement issues and therefore is not acceptable.

Unauthorized Access

The following are considered forms of unauthorized access, and as such are prohibited:

- Stealing electronic files or copying them without permission.
- Browsing the private files or accounts of others.
- Attempting to access data or resources to which the individual has not been granted explicit permissions.

System Operations

The following are prohibited as they interfere with normal systems operations:

- Introducing malicious programs into the network or server (e.g., viruses, worms, Trojan horses, email bombs, etc.).
- Interfering with or denying service to any user or system/resource.
- Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's session.
- Performing unauthorized activities that may degrade the performance of systems, such as:
- Playing electronic games
- Downloading large files, streaming music or video from the internet

Exhibit E

- Storing or downloading music, videos, and/or pictures on your computer

Unethical Behavior

The following activities are considered unethical, and are therefore prohibited at CalSAWS:

- Promoting or maintaining a personal or private business, or otherwise using CalSAWS assets or information for personal gain.
- Engaging in financial transactions such as online gambling, using CalSAWS assets or information.

Email and Other Forms of Communication

The following activities, as they relate to use of email and other forms of communication, are prohibited:

- Sending unsolicited email messages, including the sending of chain letters, "junk mail," or other advertising material or mass mailings to individuals who did not specifically request such material (email spam).
- Sending or arranging to receive information that violates state or federal laws.
- Sending any material that may defame, libel, abuse, embarrass, tarnish, present a bad image of, or portray in false light, CalSAWS, The organizations in CalSAWS, the recipient, the sender, or any other person.
- Sending pornographic, racist, or other material that is generally considered offensive.
- Sending malicious code.
- Forging email header information.
- Soliciting email for any other email address (e.g., registering another user to receive junk mail).
- Sending anonymous emails.
- Distributing or posting non-public CalSAWS information (e.g., Sensitive Information) of any kind outside of CalSAWS, without proper authorization by a CalSAWS manager.

Hardware and Software Acceptable Use

Personnel must only use hardware and software that is supplied by the project or is otherwise authorized by their supervisor or CalSAWS Technical Support. Supervisors thatdo not know if hardware/software should be authorized must consult CalSAWS Technical Support or the CalSAWS Security Officer.

Installing or executing programs on CalSAWS systems or hardware without authorization, including but not limited to, those from CDs/DVDs, audio/video streaming software or files, file shares, floppies, or downloaded from the Internet, is prohibited.

Security Requirements for Project Staff

Exhibit E

- CalSAWS Production Data (in any format) may not leave the project site unless properly secured and then only for the purpose of transfer to a location authorized by the CalSAWS Project Manager
- CalSAWS Production Data may be transported electronically ONLY by secure FTP, CalSAWS SharePoint or by encrypted email. You MAY NOT USE unencrypted email or Instant Messenger applications to transfer data.
- All printed Production data/material must be shredded or stored in a locked cabinet on the premises at all times.
- Making electronic copies of production data for the purposes for unauthorized usage is prohibited
- Transmission of production data by fax is prohibited

Laptops and Portable Data Storage Devices

Personal and Sensitive Information must be encrypted and/or password protected on any laptop, CalSAWS or otherwise. Client Sensitive Information is only allowed on CalSAWS or encrypted portable storage devices such as memory sticks and external USB drives or such devices as CalSAWS permits outside vendors and contractors to utilize in the performance of CalSAWS-related work.

Contact

Questions related to this Policy can be addressed to CalSAWS Technical Support by calling or emailing Tech.Support@CalSAWS.org, or CalSAWS Information and Privacy Security Office at Consortium.Tech.Security@CalSAWS.org.

1.2 Referenced Documents

A. CalSAWS Information Security Policy

I HAVE READ THIS AGREEMENT AND HAVE TAKEN DUE TIME TO CONSIDER IT PRIOR TO SIGNING. I UNDERSTAND THIS ENTIRE CALIFORNIA STATEWIDE AUTOMATED WELFARE SYSTEM USER SECURITY AND ACCEPTABLE USE POLICY AND AGREE TO ABIDE BY ALL OF ITS PROVISIONS:

Employee or Contractor/Vendor

NAME ____

TITLE ____

SIGNATURE ____________________________________

DATE ____

Exhibit F

County Information Technology User Responsibility Statement for Third Parties

Agreement Between Contractor: Exemplar Human Services, LLC. And County of Santa Clara Department of Employment and Benefits Services

1. DEFINITIONS

a. *"County Confidential Information"* is all material non-public information, written or oral, disclosed, directly or indirectly, through any means of communication or observation by County to Contractor or any of its affiliates or representatives

b. *"County Systems"* include but are not limited to, all County-owned, leased or managed servers, mainframe computers, desktop computers, laptop computers, handheld devices (including smart phones, wireless PDAs and Pocket PCs), equipment, networks, application systems, databases, software, phone systems, any device with network capabilities (e.g., a workstation with an attached modem, routers, switches, laptop computers, handheld devices), and any other system that stores, processes, and/or transmits County-owned information/data. These items are typically under the direct control and management of the County. "County Systems" also include these items when they are under the control and management of a service provider for use by County, as well as any personally-owned device that an individual has express written permission to use for County purposes.

c. "County-owned information/data," for purposes of this Exhibit is any information or data that is transported across a County network, or that resides in a County-owned information system, or on a network or system under the control and management of a service provider for use by County. This information/data is the exclusive property of County unless constitutional provision, State or Federal statute or case law provide otherwise. County-owned information/data does not include a User's personal, non-County business information, communications, data, files and/or software transmitted by or stored on a personally-owned device if that information/data is not transported across a County network or does not reside in a County System or on a network or system under the control and management of a service provider for use by County.

d. *"Mobile Device"* is any portable computing device that fits one of the following categories: laptops, smartphones, or tablets. "Mobile Device" does not include devices that are used exclusively for the purpose of making telephone calls.

e. *"Users"* include all employees, agents and/or representatives of Contractor performing services under this Agreement.

2. GENERAL REQUIREMENTS

a. Contractor will provide Users with a written copy of this Exhibit and will ensure that Users know, understand and comply with the requirements of this Exhibit. Users allowed access to County resources shall sign the Acknowledgement and Receipt. In all cases, such access shall be subject to approval by an authorized County representative.

b. Users are personally responsible for knowing and understanding these requirements, and are personally responsible for any actions they take that do not comply with County

Exhibit F

policies and standards. If a User is unclear as to requirements, User shall ask County for guidance.

c. If a User is issued an account for a County System, User shall comply with the following County standards for password definition, use, and management:
   1) Minimum password length is 12 characters unless a particular County System has a different requirement or is not technically feasible.
   2) The password must be high complexity (contains one of each, upper, lower, number, symbol).
   3) The password must be rotated every 90 days.
   4) User must not reuse the last 10 passwords.
   5) Access to County System is denied after 5 failed logon attempts.

d. Only authorized County staff may attach any form of computer equipment to a County network or system. This includes, but is not limited to, attachment of such devices as mobile devices, peripherals (e.g., external hard drives, printers), and USB storage media. It excludes County wireless networks provided specifically for the use of guests or visitors to County facilities.

e. User shall not use USB storage media on any County System. All such devices shall be County-owned, formally issued to User by County, and used only for legitimate County purposes.

f. User shall not connect County-owned computing equipment, including USB storage media, to non-County systems or networks, unless County gives its express written permission. This formal approval process ensures that the non-County system or network in question has been evaluated for compliance with County security standards. An example of a permitted connection to a non-County system or network would be approved connection of a County issued laptop to a home network.

g. User shall not install, configure, or use any device intended to provide connectivity to a non-County network or system (such as the Internet), on any County System, without County's express written permission. If authorized to install, configure or use such a device, User shall comply with all applicable County standards designed to ensure the privacy and protection of data, and the safety and security of County Systems. Any allowed installation shall not be activated until it is reviewed and approved in writing by an authorized County representative.

h. The unauthorized implementation or configuration of encryption, special passwords, biometric technologies, or any other methods to prevent access to County resources by those individuals who would otherwise be legitimately authorized to do so is prohibited.

i. Users shall not attempt to elevate or enhance their assigned level of privileges unless County gives its express written permission. Users who have been granted enhanced privileges due to their specific roles, such as system or network administrators, shall not abuse these privileges and shall use such privileges only in the performance of appropriate, services performed under this Agreement.

Exhibit F

j. Users shall use County-approved authentication mechanisms when accessing County networks and systems, and shall not deactivate, disable, disrupt, or bypass (or *attempt* to deactivate, disable, disrupt, or bypass) any security measure or security configuration implemented by County.

k. Users shall not circumvent, or attempt to circumvent, legal guidelines on software use and licensing. If a User is unclear as to whether a software program may be legitimately copied or installed, it is the responsibility of the User to check with County.

l. All software on County Systems shall be installed by authorized County support staff except as provided in this Agreement. Users may not download or install software on any County system unless express written permission has been obtained from County such as in this Agreement.

m. Users shall immediately report to the County TechLink Center the loss or theft of County-owned computer equipment, or of personally-owned computer equipment that has been approved for use in conducting County business or performing services under a Supplemental Agreement. The County Service Desk contact information is (408) 970-2222 or support@tss.sccgov.org.

n. Users must be aware of security issues and shall immediately report incidents to the County Information Security Office involving breaches of the security of County Systems or breaches of County-owned information/data, such as the installation of an unauthorized device, or a suspected software virus or other occurrences of malicious software or content. The Information Security Office's contact information is cybersecurityteam@iso.sccgov.org.

o. Users shall respect the sensitivity, privacy and confidentiality aspects of all County-owned information. In particular:

    1) Users shall not access, or attempt to access, County Systems or County-owned information/data unless specifically authorized to do so by the terms of this Agreement.
    2) If User is assigned a County account, User shall not allow unauthorized individuals to use their account; this includes the sharing of account passwords.
    3) Users shall not without County's written permission, use or disclose County-owned information/data other than in the performance of its obligations under this Agreement.
    4) Users shall take every precaution to ensure that all confidential or restricted information is protected from disclosure to unauthorized individuals.
    5) Users shall not make or store paper or electronic copies of information unless required to provide services under this Agreement.
    6) Users shall comply with all confidentiality requirements in Contractor's Agreement with the County. Users shall not use or disclose County Confidential Information other than in the performance of its obligations for County. All County Confidential Information shall remain the property of the County. User shall not acquire any ownership interest in County Confidential Information.

Exhibit F

p. Users shall do all of the following:
  1) Users shall not change or delete County-owned information/data unless performing such changes is required to perform services under this Agreement.
  2) Users shall avoid actions that might introduce malicious software, such as viruses or worms, onto any County system or network.
  3) Upon termination or expiration of this Agreement, Users shall not retain, give away, or remove any County-owned information/data or document from any County System or County premises. Users shall return to County all County-owned assets, including hardware and data.

q. Electronic information transported across any County network, or residing in any County System, is potentially subject to access by County technical support staff, other County personnel, and the general public. Users should not presume any level of privacy for data transmitted over a County network or stored on a County System.

r. Users must protect, respect and not infringe upon all intellectual property rights, including but not limited to rights associated with patents, copyrights, trademarks, trade secrets, proprietary information, County Confidential Information, and confidential information belonging to any other third party.

s. All information resources on any County System are the property of County and are therefore subject to County policies regarding acceptable use. No User may use any County System or County-owned information/data for the following purposes:
  1) Personal profit, including commercial solicitation or conducting or pursuing their own business interests or those of another organization that are not related to the User conducting County business. This prohibition does not apply to User’s performance of contractual obligations for the County.
  2) Unlawful or illegal activities, including downloading licensed material without authorization, or downloading copyrighted material from the Internet without the publisher’s permission.
  3) To access, create, transmit, print, download or solicit material that is, or may be construed to be, harassing or demeaning toward any individual or group for any reason, including but not limited to on the basis of sex, age, race, color, national origin, creed, disability, political beliefs, organizational affiliation, or sexual orientation, unless doing so is legally permissible and necessary in the course of conducting County business.
  4) To access, create, transmit, print, download or solicit sexually-oriented messages or images, or other potentially offensive materials such as, but not limited to, violence, unless doing so is legally permissible and necessary in the course of conducting County business.
  5) Knowingly propagating or downloading viruses or other malicious software.
  6) Disseminating hoaxes, chain letters, or advertisements.

Exhibit F

3. INTERNET AND EMAIL

a. Users shall not use County Systems for personal activities.

b. When conducting County business or performing services under this Agreement, Users shall not configure, access, use, or participate in any Internet-based communication or data exchange service unless express written permission has been given by County. Such services include, but are not limited to, file sharing (such as Dropbox, Box, Google OneDrive), Instant Messaging (such as AOL IM), email services (such as Hotmail and Gmail), peer-to-peer networking services (such as Kazaa), and social networking services (such as blogs, Instagram, Snapchat, MySpace, Facebook and Twitter). If a User has received express written permission to access such services, User shall comply with all relevant County policies, procedures, and guidelines.

c. Users assigned a County email account must comply with the County's Records Retention and Destruction Policy.

d. Users shall not use an internal County email account assigned to another individual to either send or receive email messages.

e. Users shall not configure a County email account so that it automatically forwards messages to an external Internet email system unless County gives its express written permission.

4. REMOTE ACCESS

a. Users are not permitted to implement, configure, or use any remote access mechanism unless the County has authorized the remote access mechanism.

b. County may monitor and/or record remote access sessions, and complete information on the session logged and archived. Users have no right, or expectation, of privacy when remotely accessing County Systems or County-owned information/data. County may use audit tools to create detailed records of all remote access attempts and remote access sessions, including User identifier, date, and time of each access attempt.

c. User shall configure all computer devices used to access County resources from a remote location according to NIST 800-53 standards, or an equivalent industry standard. These include approved, installed, active, and current: anti-virus software, software or hardware-based firewall, full hard drive encryption, and any other security software or security-related system configurations that are required and approved by County.

d. Users that have been provided with a County-owned device intended for remote access use, such as a laptop or other Mobile Device, shall ensure that the device is protected from damage, access by third parties, loss, or theft. Users shall immediately report loss or theft of such devices to the County Service Desk: (408) 970-2222 or support@tss.sccgov.org.

e. Users shall protect the integrity of County Systems and County-owned information/data while remotely accessing County resources, and shall immediately report any suspected security incident or concern to the County Information Security Office at cybersecurityteam@iso.sccgov.org.

Exhibit F

f. Users shall comply with any additional remote access requirements in this Agreement such as an Exhibit on Remote Access.

5. THIRD PARTY-OWNED DEVICES

a. This Section 5 applies if County permits Users to perform services under this Agreement with devices not owned by the County ("Third-party owned device"). Third-party owned devices include devices with email and/or data storage capability (such as laptops, iPhones, iPads, Android phones and tablets, BlackBerry and other "smart" devices).

b. The third party-owned device in question shall use existing, County-approved and County-owned access/authentication systems when accessing County Systems.

c. Users shall allow County to configure third party-owned devices as appropriate to meet security requirements, including the installation of specific security software mandated by County policy.

d. Use of a third party-owned device shall comply with County policies and procedures for ensuring that software updates and patches are applied to the device according to a regular, periodic schedule on at least a monthly basis. County may verify software installations and updates.

e. Users have no expectation of privacy with respect to any County-owned communications, information, or files on any third party-owned device. User agrees that, upon request, the County may immediately access any and all work-related or County-owned information/ data stored on these devices, in order to ensure compliance with County policies.

f. Users shall adhere to all relevant County security policies and standards, just as if the third party-owned device were County property. This includes, but is not limited to, policies regarding password construction and management, physical security of the device, device configuration including full storage encryption, and hard drive and/or storage sanitization prior to disposal.

g. Users shall not make modifications of any kind to operating system configurations implemented by County on the device for security purposes, or to any hardware or software installed on the device by County.

h. Users shall treat the contract-related or County-owned communications, information or files the third-party owned device contains as County property. User shall not allow access to or use of any work-related or County-owned communications, information, or files by individuals who have not been authorized by County to access or use that data.

i. Users shall report immediately to the County Information Security Office cybersecurityteam@iso.sccgov.org, any incident or suspected incident of unauthorized access and/or disclosure of County resources, data, or networks that involve the third-party owned device, and shall report the loss or theft of the device immediately to the County Service Desk: (408) 970-2222 or support@tss.sccgov.org.

Exhibit F

6. ACKNOWLEDGEMENT AND RECEIPT

This Acknowledgement hereby incorporates the URS.

By signing below, I acknowledge that I have read and understand all sections of this URS. I also acknowledge that violation of any of its provisions may result in disciplinary action, up to and including termination of my relationship with County and/or criminal prosecution.

Have you been granted Remote Access □ Yes □ No

I have read and understand the contents of the URS regarding Remote Access and the Exhibit on Remote Access. I understand that violation of these provisions may result in disciplinary action, up to and including termination of my relationship with the County and/or criminal prosecution. I received approval from County for remote access for legitimate County business, as evidenced by the signatures below.

User Signature: Date Signed:

_______________________________________ ____________________

Print User Name:

Santa Clara County
Social Services Agency

FY 2024-2025

Exhibit G: BUDGET
Resource Table
1 of 4

Agency Name:	Exemplar Human Services, LLC
Contract Period:	Upon execution - June 30, 2025
Program Name:	Reporting Tools and Services

A Source of Funds	B FY24-25 Amount	C % of Total Funding	D Commitment Code
Social Services Agency (SSA)*	$ 595,000	100%	1
Other Funding Sourcces			
	$ -	0%	
	$ -	0%	
	$ -	0%	
	$ -	0%	
	$ -	0%	
	$ -	0%	
	$ -	0%	
Total Funding Resources**	$ 595,000	100%	

Commitment Code	
1	Firm Commitment-Already have an agreement or letter confirming funding
2	Anticipated Renewal of Existing Funding-Continuation of current year funding
3	Anticipated Resource-Projection of previous fees or donations
4	Application Pending-Application has been submitted, no confirmation at this time
5	Pre-Application-Not yet submitted and expect funding

* The **SSA** line in **FY 24-25 Amount,** Column "B" should equal the **Grand Total** of Column "B" in the Budget Detail.

** The **Total Funding Resources** in Column "B" should equal the **Grand Total** of Column "D" in the Budget Detail.

FY 2024-2025

Exhibit G: BUDGET
Budget Detail (FY24)
2 of 4

Agency Name: Exemplar Human Services, LLC
Contract Period: Upon execution - June 30, 2024
Program Name: Reporting Tools and Services

A **Contracted Service***	B **Rate**	C **Est. Quantity***	D **Total**
Reporting Tools and Services	$ 35,000.00	5	$ 175,000
			$ -
			$ -
			$ -
Grand Total			**$ 175,000**

FY 2024-2025

Exhibit G: BUDGET
Budget Detail (FY25)
3 of 4

Agency Name: Exemplar Human Services LLC
Contract Period: July 1, 2024 - June 30, 2025
Program Name: Reporting Tools and Services

A **Contracted Service***	B **Rate**	C **Est. Quantity***	D **Total**
Reporting Tools and Services	$ 35,000.00	12	$ 420,000
			$ -
			$ -
			$ -
Grand Total			**$ 420,000**

Agency Name:	Exemplar Human Services, LLC
Contract Period:	Upon execution - June 30, 2025
Program Name:	Reporting Tools and Services

Please provide detail for each line item. Narrative should explain each service, including the ancillary services that are included as part of the primary service. All ancillary services listed in the Outputs section of your Work Plan, but not included as a budget line item, should be included in the Narrative for the line item to which it corresponds.

Contracted Service(s)*	Narrative
Reporting Tools and Services	Contractor to provide a portfolio of reporting tools to assist DEBS staff with workload and in meeting service and performance outcomes.

***Contracted Services rate always include all direct, indirect, and administrative costs related to providing the services. This includes, but is not limited to, personnel cost, travel, technology, training, curriculum development or acquisition costs, support staff, management, credentialing, and quality improvement and/or quality assurance.**

Logic Model - Reporting Tools and Services

Agency Name: Exemplar Human Services, LLC

A. Contract Goal: Contract to provide reporting tools and services to DEBS as a staff resource and to aid in meeting service and performance outcomes.

B. Situation	C. Activities/Services	D1. # of unduplicated clients/families served per FY	D2. # of Outputs per FY	D3. Output	E. Short/Long Term Outcome Measures
DEBS is having challenges with getting adequate reporting tools and data from CalSAWS system. Reporting and data is needed to meet service requirements and to ensure performance standards are met.	Intake Productivity Report	N/A Clients	All Benefit Services Staff	Daily	Reports will be received by DEBS staff daily, 98% of time.
	Continuing Productivity Report		All Benefit Services Staff	Daily	
	WtW Productivity Report		All Employment Staff	Daily	Power Business Intelligence Site is available between 7:00 AM and 6:00 PM Pacific, 98% of time.
	Productivity/Tele-work Report		All DEBS Staff	Daily	
	Intake Pending Apps Report		All Benefit Services Staff	Daily	Data validation issues resolved within 24 hours, 98% of time.
	Continuing Eligibility Report		All Benefit Services Staff	Daily	
	Welfare to Work Alerts Report		All Employment Staff	Daily	
	Executive Dashboard		All DEBS Executives	Monthly	
	Power Business Intelligence (PBI) Suite		All DEBS Staff	Daily	