AGREEMENT

BETWEEN

COUNTY OF ORANGE

AND

ACCESS CALIFORNIA SERVICES

FOR THE PROVISION OF REFUGEE SOCIAL SERVICES

AND

REFUGEE HEALTH SERVICES

This AGREEMENT, entered into this 1st day of October 2017, which date is particularized for purpose of reference only, is by and between the COUNTY OF ORANGE, hereinafter referred to as "COUNTY," and ACCESS CALIFORNIA SERVICES, a California non-profit corporation, hereinafter referred to as "CONTRACTOR." This Agreement shall be administered by the County of Orange Social Services Agency Director or designee, hereinafter referred to as "ADMINISTRATOR" or "SSA." Direct services of Exhibit B shall be administered by the County of Orange Health Care Agency, hereinafter referred to as "HCA."

W I T N E S S E T H:

WHEREAS, CONTRACTOR agrees to render such services on the terms and conditions hereinafter set forth;

WHEREAS, such services are authorized and provided for pursuant to the Immigration and Nationality Act, as amended by the Federal Refugee Education Assistance Act of 1980, Title V, Section 501(a), Public Law 96-422, 94 Stat. 1799, 8 U.S.C 1522 note; Refugee Act of 1980, Section 412, Public Law 96-212, 94 Stat. 111, 8 U.S.C 1522; William Wilberforce Trafficking Victims Protection Reauthorization Act of 2008, Section 212-235, Public Law 110-457; Victims of

Trafficking and Violence Protection Act of 2000, Public Law 106-386; and

WHEREAS, Section 13275 et seq., of the Welfare and Institutions Code provides for funds derived from the Federal Refugee Act of 1980 to be used to provide employment services for refugees.

NOW, THEREFORE, IT IS MUTUALLY AGREED AS FOLLOWS:

///

///

///

///

///

///

///

///

///

///

///

///

///

///

///

///

///

///

///

///

///

///

TABLE OF CONTENTS

1. TERM

The term of this Agreement shall commence on October 1, 2017, and terminate on September 30, 2020, unless earlier terminated pursuant to the provisions of Paragraph 42 of this Agreement; however, CONTRACTOR shall be obligated to perform such duties as would normally extend beyond this term, including but not limited to, obligations with respect to indemnification, audits, reporting and accounting. CONTRACTOR and ADMINISTRATOR may mutually agree in writing to extend the term of this Agreement, for up to twelve (12) additional months upon the same terms and conditions, provided that COUNTY's maximum obligation as stated in Subparagraph 19.1 of this Agreement does not increase as a result.

2. ALTERATION OF TERMS

This Agreement, including any Exhibit(s) attached hereto and incorporated by reference, fully expresses all understandings of the parties and is the total Agreement between the parties as to the subject matter of this Agreement. No addition to, or alteration of, the terms of this Agreement, whether written or verbal, by the parties, their officers, agents or employees, are valid or binding unless made in the form of a written amendment to this Agreement which is formally approved and executed by both parties.

3. STATUS OF CONTRACTOR

3.1 CONTRACTOR is and shall at all times be deemed to be an independent contractor and shall be wholly responsible for the manner in which it performs the services required of it by the terms of this Agreement. Nothing herein contained shall be construed as creating the relationship of employer and employee, or principal and agent, between COUNTY and CONTRACTOR or any of CONTRACTOR's agents or employees. CONTRACTOR assumes exclusively the responsibility for the acts of its employees or agents as they relate to

services to be provided during the course and scope of their employment.

3.2 CONTRACTOR, its agents, employees and volunteers shall not be entitled to any rights and/or privileges of COUNTY employees and shall not be considered in any manner to be COUNTY employees.

4. DESCRIPTION OF SERVICES, STAFFING

4.1 CONTRACTOR agrees to provide those services, facilities, equipment and supplies as described in the Exhibits to the Agreement between County of Orange and Access California Services, for the Provision of Refugee Social Services and Refugee Health Services, attached hereto and incorporated herein by reference. Exhibit "A" relating to Refugee Social Services, Exhibit "B" relating to Refugee Health Services. CONTRACTOR shall operate continuously throughout the term of this Agreement with the number and type of staff described and as required for provision of services hereunder.

4.2 Subject to thirty (30) days advance written notice, ADMINISTRATOR may require changes in staffing allocations to reflect current workload demands or service needs as long as COUNTY's maximum obligation as set forth in this Agreement is not exceeded.

4.3 Upon the request of ADMINISTRATOR, CONTRACTOR shall send appropriate staff to attend an orientation session and subsequent training sessions given by COUNTY.

5. LICENSES AND STANDARDS

5.1 CONTRACTOR warrants that it has all necessary licenses and permits required by the laws of the United States, State of California, County of Orange and all other appropriate governmental agencies to perform the services described in this Agreement, and agrees to maintain these licenses and permits in effect for the duration of this Agreement. Further, CONTRACTOR warrants that its employees shall conduct themselves in compliance with such laws and licensure requirements including, without limitation, compliance with laws

applicable to sexual harassment and ethical behavior.

5.2 In the performance of this Agreement, CONTRACTOR shall comply with all applicable provisions of the California Welfare and Institutions Code (WIC); Title 45 of the Code of Federal Regulations (CFR); implementing regulations under 2 CFR Part 200, Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards; Title 48 CFR Section 31.2; and all applicable laws and regulations of the United States, State of California, County of Orange Social Services Agency and all administrative regulations, rules and policies adopted thereunder as each and all may now exist or be hereafter amended.

5.2.1 For Federally funded Agreements in the amount of $25,000 or more, CONTRACTOR certifies that its officers and/or principals are not debarred or suspended from Federal financial assistance programs and/or activities

6. DELEGATION AND ASSIGNMENT/SUBCONTRACTS

6.1 Delegation and Assignment:

In the performance of this Agreement, CONTRACTOR may neither delegate its duties or obligations nor assign its rights, either in whole or in part, without the prior written consent of COUNTY. Any attempted delegation or assignment without prior written consent shall be void. The transfer of assets in excess of ten percent (10%) of the total assets of CONTRACTOR, or any change in the corporate structure, the governing body, or the management of CONTRACTOR, which occurs as a result of such transfer, shall be deemed an assignment of benefits under the terms of this Agreement requiring COUNTY approval.

6.2 Subcontracts:

CONTRACTOR shall not subcontract for services under this Agreement without the prior written consent of ADMINISTRATOR. If ADMINISTRATOR consents

in writing to a subcontract, in no event shall the subcontract alter, in any way, any legal responsibility of CONTRACTOR to COUNTY. All subcontracts must be in writing and copies of same shall be provided to ADMINISTRATOR. CONTRACTOR shall include in each subcontract any provision ADMINISTRATOR may require.

6.2.1 Subcontracts of $25,000 or less:

CONTRACTOR shall develop a standard form Purchase Order, subject to prior written approval of ADMINISTRATOR, to be utilized for the purchase of services by CONTRACTOR when the cumulative total cost of the services to be provided by any organization is anticipated to be twenty-five thousand dollars ($25,000) or less during the term of this Agreement. The basis for costs incurred by any such Purchase Order(s) shall be the actual cost of providing services or the usual and customary charges established by the organization(s) providing the services.

6.2.2 Subcontracts in excess of $25,000:

CONTRACTOR shall develop and submit for approval to ADMINISTRATOR a system for the procurement of subcontracts with any organization in which the total cumulative cost of services provided by any single organization is anticipated to exceed twenty-five thousand dollars ($25,000) during the term of this Agreement. CONTRACTOR's proposed procurement system shall take into consideration such factors as: degree of price competition; pricing policies and techniques; experience and quality of service; methods of evaluating subcontractor responsibility; relationship of subcontractor to CONTRACTOR; and planning, award, and post-award management of subcontracts, including internal audit procedures and monitoring of subcontractor's performance until completion of services.

Upon ADMINISTRATOR's approval of CONTRACTOR's proposed procurement system, CONTRACTOR shall comply with such procurement system in

obtaining subcontracts with a total cost in excess of twenty-five thousand dollars ($25,000) during the term of this Agreement. In addition, CONTRACTOR shall obtain ADMINISTRATOR's written consent prior to entering into a subcontract with any organization when the total cumulative cost of services to be provided by that organization is anticipated to exceed twenty-five thousand dollars ($25,000) during the term of this Agreement.

CONTRACTOR and its subcontractor(s) shall establish and maintain accurate and complete financial records related to services provided under the terms of this Agreement. Such records may be subject to the satisfaction of ADMINISTRATOR, and to the examination and audit by ADMINISTRATOR or designee, for a period of five (5) years, or until any pending audit is completed.

7. FORM OF BUSINESS ORGANIZATION AND REAL PROPERTY DISCLOSURE

7.1 Form of Business Organization:

Upon the request of ADMINISTRATOR, CONTRACTOR shall prepare and submit, within thirty (30) days thereafter, an affidavit executed by persons satisfactory to ADMINISTRATOR containing, but not limited to, the following information:

7.1.1 The form of CONTRACTOR's business organization, i.e., proprietorship, partnership, corporation, etc.

7.1.2 A detailed statement indicating the relationship of CONTRACTOR, by way of ownership or otherwise, to any parent organization or individual.

7.1.3 A detailed statement indicating the relationship of CONTRACTOR to any subsidiary business organization or to any individual who may be providing services, supplies, material or equipment to CONTRACTOR or in any manner does business with CONTRACTOR under this Agreement.

///

7.2 Change in Form of Business Organization:

If during the term of this Agreement the form of CONTRACTOR's business organization changes, or the ownership of CONTRACTOR changes, or CONTRACTOR's relationship to other businesses dealing with CONTRACTOR under this Agreement changes, CONTRACTOR shall promptly notify ADMINISTRATOR, in writing, detailing such changes. A change in the form of business organization may, at COUNTY's sole discretion, be treated as an attempted assignment of rights or delegation of duties of this Agreement.

7.3 Real Property Disclosure:

If CONTRACTOR is occupying any real property under any agreement, oral or written, where persons are to receive services hereunder, CONTRACTOR shall submit the following information in addition to a copy of the lease, license or rental agreement, as well as any other information requested, prior to the provision of services under this Agreement:

7.3.1 The location by street address and city of any such real property.

7.3.2 The fair market value of any such real property as such value is reflected on the most recently issued County Tax Collector's tax bill.

7.3.3 A detailed description of all existing and pending agreements, with respect to the use or occupation of any such real property. Such description shall include, but not be limited to:

7.3.3.1 The term duration of any rental, lease or license agreement;

7.3.3.2 The amount of monetary consideration to be paid to the lessor or licensor over the term of the rental, lease or license agreement;

7.3.3.3 The type and dollar value of any other

consideration to be paid to the lessor or licensor; and

7.3.3.4 The full names and addresses of all parties to any agreement concerning the real property and a listing of liens (if any) thereof, together with a listing by full names and addresses of all officers, directors and stockholders of any private corporation, and a similar listing of all general and limited partners of any partnership which is a party.

7.3.4 A listing by full names of all of CONTRACTOR's officers, directors and/or partners, members of its administrative and advisory boards, staff and consultants, who have any family relationship by marriage or blood with a party to any agreement concerning real property referred to in Subparagraph 7.3.3, immediately above, or who have any present or future financial interest in such person's business, whether the entity concerned is a corporation or partnership. Such listing shall also include the full names of all of CONTRACTOR's officers, directors, partners and those holding a financial interest. Included are members of its advisory boards, members of its staff and consultants, who have any family relationship by marriage or blood to an officer, director, or stockholder of the corporation or to any partner of the partnership. In preparing the latter listing, CONTRACTOR shall also indicate the names of the officers, directors, stockholders, or partner(s), as appropriate, and the family relationship which exists between such person(s) and CONTRACTOR's representatives listed.

7.3.5 True and correct copies of all agreements with respect to any such real property shall be appended to the documentation described above and made a part thereof. If, during the term of this Agreement, there is a change in the agreement(s) with respect to real property where persons receive services, CONTRACTOR shall promptly notify ADMINISTRATOR, in writing, describing such changes.

///

8. NON-DISCRIMINATION

8.1 In the performance of this Agreement, CONTRACTOR agrees that it shall not engage nor employ any unlawful discriminatory practices in the admission of CLIENTs, provision of services or benefits, assignment of accommodations, treatment, evaluation, employment of personnel or in any other respect on the basis of race, religious creed, color, national origin, ancestry, physical disability, mental disability, medical condition, genetic information, marital status, sex, gender, gender identity, gender expression, age, sexual orientation, military and veteran status or any other protected group in accordance with the requirements of all applicable Federal or State laws.

8.2 CONTRACTOR shall develop an Affirmative Action Program Plan which meets the lawful and applicable requirements of the U.S. Department of Health and Human Services.

8.3 CONTRACTOR shall furnish any and all information requested by ADMINISTRATOR and shall permit ADMINISTRATOR access, during business hours, to books, records and accounts in order to ascertain CONTRACTOR's compliance with Paragraph 8 et seq.

8.4 CONTRACTOR shall comply with Executive Order 11246, entitled "Equal Employment Opportunity," as amended by Executive Order 11375 and as supplemented in Department of Labor regulations (Title 41 CFR Part 60).

8.5 Non-Discrimination in Employment:

8.5.1 All solicitations or advertisements for employees placed by or on behalf of CONTRACTOR shall state that all qualified applicants will receive consideration for employment without regard to race, religious creed, color, national origin, ancestry, physical disability, mental disability, medical condition, genetic information, marital status, sex, gender, gender identity, gender expression, age, sexual orientation, military and veteran

status or any other protected group in accordance with the requirements of all applicable Federal or State laws. Notices describing the provisions of the equal opportunity clause shall be posted in a conspicuous place for employees and job applicants.

8.5.2 CONTRACTOR shall refer any and all employees desirous of filing a formal discrimination complaint to:

California Department of Social Services
Public Inquiry and Response Bureau
P.O. Box 944243, M.S. 8-4-23
Sacramento, CA 95814
Telephone: (800) 952-5253
(800) 952-8349 (For the hard of hearing)

8.6 Non-Discrimination in Service Delivery:

8.6.1 CONTRACTOR shall comply with Titles VI and VII of the Civil Rights Act of 1964, as amended; Section 504 of the Rehabilitation Act of 1973, as amended; the Age Discrimination Act of 1975, as amended; the Food Stamp Act of 1977, as amended, and in particular 7 CFR section 272.6; Title II of the Americans with Disabilities Act of 1990, as amended; California Civil Code Section 51 et seq., as amended; California Government Code (CGC) Sections 11135-11139.5, as amended; CGC Section 12940 (c), (h), (i), and (j); CGC Section 4450; Title 22, California Code of Regulations (CCR) Sections 98000-98413; the Dymally-Alatorre Bilingual Services Act (CGC Section 7290-7299.8); Section 1808 of the Removal of Barriers to Interethnic Adoption Act of 1996; and other applicable Federal and State laws, as well as their implementing regulations (including Title 45 CFR Parts 80, 84, and 91; Title 7 CFR Part 15; and Title 28 CFR Part 42), and any other law pertaining to Equal Employment Opportunity, Affirmative Action and Nondiscrimination as each may now exist or be hereafter amended. CONTRACTOR shall not implement any administrative

methods or procedures which would have a discriminatory effect or which would violate the California Department of Social Services (CDSS) Manual of Policies and Procedures (MPP) Division 21, Chapter 21-100. If there are any violations of this Paragraph, CDSS shall have the right to invoke fiscal sanctions or other legal remedies in accordance with WIC Section 10605, or CGC Sections 11135-11139.5, or any other laws, or the issue may be referred to the appropriate Federal agency for further compliance action and enforcement of Subparagraph 8.6 et seq.

8.6.2 CONTRACTOR shall provide any and all CLIENTs desirous of filing a formal complaint any and all information as appropriate:

8.6.2.1 Pamphlet: "Your Rights Under California Welfare Programs" (PUB 13)

8.6.2.2 Discrimination Complaint Form

8.6.2.3 Civil Rights Contacts:

County Civil Rights Contact:
Orange County Social Services Agency
Program Integrity
Attn: Civil Rights Coordinator
P.O. Box 22001
Santa Ana, CA 92702-2001
Telephone: (714) 438-8877

State Civil Rights Contact:
California Department of Social Services
Civil Rights Bureau
P.O. Box 944243, M.S. 15-70
Sacramento, CA 94244-2430

Federal Civil Rights Contact:
U.S. Department of Health and Human Services

Office of Civil Rights
50 U.N. Plaza, Room 322
San Francisco, CA 94102

9. NOTICES

9.1 All notices, requests, claims, correspondence, reports, statements authorized or required by this Agreement, and/or other communications shall be addressed as follows:

COUNTY: County of Orange Social Services Agency
Contracts and Procurement Services
500 N. State College Blvd, Suite #100
Orange, CA 92868

CONTRACTOR: Access California Services
631 S. Brookhurst Street Suite 107
Anaheim, CA 92804

9.2 All notices shall be deemed effective when in writing and deposited in the United States mail, first class, postage prepaid and addressed as above. Any notices, claims, correspondence, reports and/or statements authorized or required by this Agreement addressed in any other fashion shall be deemed not given. The Parties each may designate by written notice from time to time, in the manner aforesaid, any change in the address to which notices must be sent.

10. NOTICE OF DELAYS

Except as otherwise provided under this Agreement, when either party has knowledge that any actual or potential situation is delaying or threatens to delay the timely performance of this Agreement, that party shall, within one (1) business day, give notice thereof, including all relevant information with respect thereto, to the other party.

11. INDEMNIFICATION

11.1 CONTRACTOR agrees to indemnify, defend with counsel approved in writing by COUNTY, and hold U.S. Department of Health and Human Services, the State, COUNTY, and their elected and appointed officials, officers, employees, agents and those special districts and agencies which COUNTY's Board of Supervisors acts as the governing Board ("COUNTY INDEMNITEES") harmless from any claims, demands or liability of any kind or nature, including but not limited to personal injury or property damage, arising from or related to the services, products or other performance provided by CONTRACTOR pursuant to this Agreement. If judgment is entered against CONTRACTOR and COUNTY by a court of competent jurisdiction because of the concurrent active negligence of COUNTY or COUNTY INDEMNITEES, CONTRACTOR and COUNTY agree that liability will be apportioned as determined by the court. Neither party shall request a jury apportionment.

12. INSURANCE

12.1 Prior to the provision of services under this Agreement, CONTRACTOR agrees to purchase all required insurance at CONTRACTOR's expense and to deposit with ADMINISTRATOR Certificates of Insurance, including all endorsements required herein, necessary to satisfy COUNTY that the insurance provisions of this Agreement have been complied with. CONTRACTOR agrees to keep such insurance coverage, Certificates of Insurance and endorsements on deposit with ADMINISTRATOR during the entire term of this Agreement. In addition, all subcontractors performing work on behalf of CONTRACTOR pursuant to this Agreement shall obtain insurance subject to the same terms and conditions as set forth herein for CONTRACTOR.

12.2 CONTRACTOR shall ensure that all subcontractors performing work on behalf of CONTRACTOR pursuant to this Agreement shall be covered under CONTRACTOR's insurance as an Additional Insured or maintain insurance subject

to the same terms and conditions as set forth herein for CONTRACTOR. CONTRACTOR shall not allow subcontractors to work if subcontractors have less than the level of coverage required by COUNTY from CONTRACTOR under this Agreement. It is the obligation of CONTRACTOR to provide notice of the insurance requirements to every subcontractor and to receive proof of insurance prior to allowing any subcontractor to begin work. Such proof of insurance must be maintained by CONTRACTOR through the entirety of this Agreement for inspection by COUNTY representative(s) at any reasonable time.

12.3 All self-insured retentions (SIRs) shall be clearly stated on the Certificate of Insurance. Any self-insured retention (SIR) in an amount in excess of fifty thousand dollars ($50,000) shall specifically be approved by the COUNTY's Risk Manager, or designee, upon review of CONTRACTOR's current audited financial report. If CONTRACTOR's SIR is approved, CONTRACTOR, in addition to, and without limitation of, any other indemnity provision(s) in the Agreement, agrees to all of the following:

12.3.1 In addition to the duty to indemnify and hold COUNTY harmless against any and all liability, claim, demand or suit resulting from CONTRACTOR's, its agent's, employee's or subcontractor's performance of this Agreement, CONTRACTOR shall defend COUNTY at its sole cost and expense with counsel approved by Board of Supervisors against same; and

12.3.2 CONTRACTOR's duty to defend, as stated above, shall be absolute and irrespective of any duty to indemnify or hold harmless; and

12.3.3 The provisions of California Civil Code Section 2860 shall apply to any and all actions to which the duty to defend stated above applies, and CONTRACTOR'S SIR provisions shall be interpreted as though CONTRACTOR was an insurer and COUNTY was the insured.

12.4 If CONTRACTOR fails to maintain insurance acceptable to COUNTY for the full term of this Agreement, COUNTY may terminate this Agreement.

12.5 Qualified Insurer:

12.5.1 Minimum insurance company ratings as determined by the most current edition of the Best's Key Rating Guide/Property-Casualty/United States shall be A- (Secure A.M. Best's Rating) and VIII (Financial Size Category).The policy or policies of insurance required herein must be issued by an insurer with a minimum rating of A- (Secure A.M. Best's Rating) and VIII (Financial Size Category as determined by the most current edition of the Best's Key Rating Guide/Property-Casualty/United States or ambest.com). It is preferred, but not mandatory, that the insurer be licensed to do business in the state of California (California Admitted Carrier).

12.6 If the insurance carrier does not have an A.M. Best Rating of A-/VIII, the CEO/Office of Risk Management retains the right to approve or reject a carrier after a review of the company's performance and financial rating.

12.7 The policy or policies of insurance maintained by CONTRACTOR shall provide the minimum limits and coverage as set forth below:

Coverage	Minimum Limits
Commercial General Liability	$1,000,000 per occurrence $2,000,000 aggregate
Automobile Liability including coverage for owned, non-owned and hired vehicles	$1,000,000 per occurrence
Passenger Vehicles up to four (4) passengers, not including the driver	$1,000,000 per occurrence
Passenger Vehicles up to seven (7) passengers, not including the driver	$2,000,000 per occurrence
Passenger Vehicles for eight (8) or more passengers, not including the driver	$5,000,000 per occurrence
Workers' Compensation	Statutory

Employer's Liability Insurance	$1,000,000 per occurrence
Network Security & Privacy Liability	$1,000,000 per claims made
Professional Liability Insurance	$1,000,000 per claims made $1,000,000 aggregate
Sexual Misconduct Liability	$1,000,000 per occurrence

12.8 Required Coverage Forms:

12.8.1 Commercial General Liability coverage shall be written on Insurance Services Office (ISO) form CG 00 01 or a substitute form providing liability coverage at least as broad.

12.8.2 Business Auto Liability coverage shall be written on ISO form CA 00 01, CA 00 05, CA 0012, CA 00 20 or a substitute form providing coverage at least as broad.

12.9 Required Endorsements:

12.9.1 Commercial General Liability policy shall contain the following endorsements, which shall accompany the Certificate of Insurance:

12.9.1.1 An Additional Insured endorsement using ISO form CG 20 26 04 13, or a form at least as broad, naming the County of Orange, its elected and appointed officials, officers, agents and employees, as Additional Insureds or provide blanket coverage, which will state AS REQUIRED BY WRITTEN CONTRACT.

12.9.1.2 A primary non-contributing endorsement using ISO form CG 20 01 04 13, or a form at least as broad, evidencing that CONTRACTOR's insurance is primary and any insurance or self-insurance maintained by the County of Orange shall be excess and non-contributing.

12.9.2 The Network Security and Privacy Liability policy shall contain the following endorsements which shall accompany the Certificate of

Insurance.

12.9.2.1 An Additional Insured endorsement naming the County of Orange, its elected and appointed officials, officers, agents and employees as Additional Insureds for its vicarious liability.

12.9.2.2 A primary and non-contributing endorsement evidencing that the CONTRACTOR's insurance is primary and any insurance or self-insurance maintained by the County of Orange shall be excess and non-contributing.

12.10 The Workers' Compensation policy shall contain a waiver of subrogation endorsement waiving all rights of subrogation against the County of Orange, its elected and appointed officials, officers, agents and employees or provide blanket coverage, which will state AS REQUIRED BY WRITTEN CONTRACT.

12.11 All insurance policies required by this Agreement shall waive all rights of subrogation against the County of Orange, its elected and appointed officials, officers, agents and employees when acting within the scope of their appointment or employment.

12.12 CONTRACTOR shall notify COUNTY in writing within thirty (30) days of any policy cancellation and ten (10) days for non-payment of premium and provide a copy of the cancellation notice to COUNTY. Failure to provide written notice of cancellation may constitute a material breach of the contract, upon which the COUNTY may suspend or terminate this Agreement.

12.13 If CONTRACTOR's Professional Liability policy is a "claims made" policy, CONTRACTOR shall agree to maintain professional liability coverage for two (2) years following completion of this Agreement.

12.14 The Commercial General Liability policy shall contain a severability of interests clause also known as a "separation of insureds" clause (standard in the ISO CG 0001 policy).

12.15 Insurance certificates should be mailed to COUNTY at the address

indicated in Paragraph 9 of this Agreement.

12.16 If CONTRACTOR fails to provide the insurance certificates and endorsements within seven (7) days of notification by CEO/County Procurement Office or ADMINISTRATOR, award may be made to the next qualified proponent.

12.17 COUNTY expressly retains the right to require CONTRACTOR to increase or decrease insurance of any of the above insurance types throughout the term of this Agreement. Any increase or decrease in insurance will be as deemed by County of Orange Risk Manager as appropriate to adequately protect COUNTY.

12.18 COUNTY shall notify CONTRACTOR in writing of changes in the insurance requirements. If CONTRACTOR does not deposit copies of acceptable certificates of insurance and endorsements with COUNTY incorporating such changes within thirty (30) days of receipt of such notice, this Agreement may be in breach without further notice to CONTRACTOR, and COUNTY shall be entitled to all legal remedies.

12.19 The procuring of such required policy or policies of insurance shall not be construed to limit CONTRACTOR's liability hereunder nor to fulfill the indemnification provisions and requirements of this Agreement, nor act in any way to reduce the policy coverage and limits available from the insurer.

13. NOTIFICATION OF INCIDENTS, CLAIMS OR SUITS

CONTRACTOR shall report to COUNTY:

13.1 Any accident or incident relating to services performed under this Agreement that involves injury or property damage which may result in the filing of a claim or lawsuit against CONTRACTOR and/or COUNTY. Such report shall be made in writing within twenty-four (24) hours of occurrence.

13.2 Any third party claim or lawsuit filed against CONTRACTOR arising from or relating to services performed by CONTRACTOR under this Agreement.

Such report shall be submitted to COUNTY within twenty-four (24) hours of occurrence.

13.3 Any injury to an employee of CONTRACTOR that occurs on COUNTY property. Such report shall be submitted to COUNTY within twenty-four (24) hours of occurrence.

13.4 Any loss, disappearance, destruction, misuse or theft of any kind whatsoever of COUNTY property, monies or securities entrusted to CONTRACTOR under the term of this Agreement. Such report shall be submitted to COUNTY within twenty-four (24) hours of occurrence.

14. CONFLICT OF INTEREST

14.1 CONTRACTOR shall exercise reasonable care and diligence to prevent any actions or conditions that could result in a conflict with the best interests of COUNTY. This obligation shall apply to CONTRACTOR and CONTRACTOR's employees, volunteers, agents, relatives, subcontractors and third parties associated with accomplishing the work hereunder.

14.2 CONTRACTOR's efforts shall include, but not be limited to, establishing precautions to prevent its employees or agents from making, receiving, providing, or offering gifts, entertainment, payments, loans or other considerations which could be deemed to appear to influence individuals to act contrary to the best interests of COUNTY.

15. ANTI-PROSELYTISM PROVISION

No funds provided directly to institutions or organizations to provide services and administer programs under Title 42 United States Code (USC) Section 604a(a)(1)(A) shall be expended for sectarian worship, instruction, or proselytization, except as otherwise permitted by law.

16. SUPPLANTING GOVERNMENT FUNDS

CONTRACTOR shall not supplant any Federal, State or COUNTY funds intended for the purposes of this Agreement with any funds made available

under this Agreement. CONTRACTOR shall not claim reimbursement from COUNTY for, or apply sums received from COUNTY with respect to, that portion of its obligations which have been paid by another source of revenue. CONTRACTOR agrees that it shall not use funds received pursuant to this Agreement, either directly or indirectly, as a contribution or compensation for purposes of obtaining Federal, State or COUNTY funds under any Federal, State or COUNTY program without prior written approval of ADMINISTRATOR.

17. EQUIPMENT

17.1 All items purchased with funds provided under this Agreement, or which are furnished to CONTRACTOR by COUNTY, which have a single unit cost of at least five thousand dollars ($5,000), including sales tax, shall be considered Capital Equipment. Title to all Capital Equipment shall, upon purchase, vest and remain in COUNTY. The use of such items of Capital Equipment is limited to the performance of this Agreement. Upon the termination of this Agreement, CONTRACTOR shall immediately return any items of Capital Equipment to COUNTY or its representatives, or dispose of them in accordance with the directions of ADMINISTRATOR.

CONTRACTOR further agrees to the following:

17.1.1 To maintain all items of Capital Equipment in good working order and condition, normal wear and tear excepted.

17.1.2 To label all items of Capital Equipment, do periodic inventories as required by ADMINISTRATOR and to maintain an inventory list showing where and how the Capital Equipment is being used, in accordance with procedures developed by ADMINISTRATOR. All such lists shall be submitted to ADMINISTRATOR within ten (10) days of any request therefore.

17.1.3 To report in writing to ADMINISTRATOR immediately after discovery, the loss or theft of any items of Capital Equipment. For stolen items, the local law enforcement agency must be contacted and a copy of the

police report submitted to ADMINISTRATOR.

17.1.4 To purchase a policy or policies of insurance covering loss or damage to any and all Capital Equipment purchased under this Agreement, in the amount of the full replacement value thereof, providing protection against the classification of fire, extended coverage, vandalism, malicious mischief and special extended perils (all risks) covering the parties' interests as they appear.

17.2 The purchase of any Capital Equipment by CONTRACTOR shall be requested in writing, shall require the prior written approval of ADMINISTRATOR, and shall fulfill the provisions of this Agreement which are appropriate and directly related to CONTRACTOR's service or activity under the terms of this Agreement. COUNTY may refuse reimbursement for any costs resulting from Capital Equipment purchased, which are incurred by CONTRACTOR, if prior written approval has not been obtained from ADMINISTRATOR.

17.3 Personal Computer Equipment:

No personal computers and/or personal electronic devices, such as tablets and laptop computers, or any component thereof may be purchased with funds provided under this Agreement, regardless of purchase price, without prior written approval of ADMINISTRATOR. Any such purchase shall be in accordance with specifications provided by ADMINISTRATOR, be subject to the same inventory control conditions specified in Subparagraphs 17.1.1 to 17.1.4 and, at the sole discretion of ADMINISTRATOR, become the property of COUNTY upon termination of this Agreement.

18. BREACH SANCTIONS

Failure by CONTRACTOR to comply with any of the provisions, covenants, or conditions of this Agreement shall be a material breach of this Agreement. In such event, ADMINISTRATOR may, and in addition to immediate termination and any other remedies available at law, in equity, or otherwise specified in this

Agreement:

18.1 Afford CONTRACTOR a time period within which to cure the breach, which period shall be established by ADMINISTRATOR; and/or

18.2 Discontinue reimbursement to CONTRACTOR for and during the period in which CONTRACTOR is in breach, which reimbursement shall not be entitled to later recovery; and/or

18.3 Offset against any monies billed by CONTRACTOR but yet unpaid by COUNTY those monies disallowed pursuant to Subparagraph 18.2 above.

ADMINISTRATOR will give CONTRACTOR written notice of any action pursuant to this Paragraph, which notice shall be deemed served on the date of mailing.

19. PAYMENTS

19.1 Maximum Contractual Obligation:

The maximum obligation of COUNTY under this Agreement shall not exceed the amount of $2,142,900: the amount of $714,300 for October 1, 2017 through September 30, 2018; the amount of $714,300 for October 1, 2018 through September 30, 2019; and the amount of $714,300 for October 1, 2019 through September 30, 2020, or actual allowable costs, whichever is less. This amount shall consist of $1,500,000 for RSS as described in Exhibit A to this Agreement; and $642,900 for RHS, as described in Exhibit B to this Agreement.

19.2 Subparagraphs 19.3 and 19.4 below shall apply only to the provisions of Exhibit A to this Agreement, and do not apply to Exhibit B to this Agreement.

19.3 Allowable Costs:

During the term of this Agreement, COUNTY shall pay CONTRACTOR monthly in arrears, for actual allowable costs incurred and paid by CONTRACTOR pursuant to this Agreement, as defined in 2 CFR, Part 230 or as approved by ADMINISTRATOR. However, COUNTY, in its sole discretion, may pay CONTRACTOR for anticipated allowable costs that will be incurred by CONTRACTOR for June

2018, June 2019, and June 2010, during the month of such anticipated expenditure.

19.4 Claims:

19.4.1 CONTRACTOR shall submit monthly claims to be received by ADMINISTRATOR no later than the twentieth (20th) calendar day of the month for expenses incurred in the preceding month. In the event the twentieth (20th) calendar day falls on a weekend or COUNTY holiday, CONTRACTOR shall submit the claim the next business day. COUNTY holidays include New Year's Day, Martin Luther King Day, President Lincoln's Birthday, Presidents' Day, Memorial Day, Independence Day, Labor Day, Columbus Day, Veterans Day, Thanksgiving Day, Friday after Thanksgiving, and Christmas Day.

19.4.2 All claims must be submitted on a form approved by ADMINISTRATOR. ADMINISTRATOR may require CONTRACTOR to submit supporting source documents with the monthly claim, including, inter alia, a monthly statement of services, general ledgers, supporting journals, time sheets, invoices, canceled checks, receipts and receiving records, some of which may be required to be copied. Source documents that CONTRACTOR must submit shall be determined by ADMINISTRATOR and/or COUNTY's Auditor-Controller. CONTRACTOR shall retain all financial records in accordance with Paragraph 24 (Records, Inspections, and Audits) of this Agreement.

19.4.3 Payments should be released by COUNTY within a reasonable time period of approximately thirty (30) days after receipt of a correctly completed claim form and required supporting documentation.

19.4.4 Year End and Final Claims:

19.4.4.1 CONTRACTOR shall submit a final claim for each fiscal year, October 1 through September 30, covered under the term of this Agreement as stated in Paragraph 1, by no later than November 30th of each corresponding fiscal year. Claims received after November 30th of each

corresponding COUNTY fiscal year may, at ADMINISTRATOR's sole discretion, not be reimbursed. ADMINISTRATOR may modify the date upon which the final claim per each COUNTY fiscal year must be received, upon written notice to CONTRACTOR.

19.4.4.2 The basis for final settlement shall be the actual allowable costs as defined in Title 45 CFR and 2 CFR, Part 230, incurred and paid by CONTRACTOR pursuant to this Agreement; limited, however, to the maximum obligation of COUNTY. In the event that any overpayment has been made, COUNTY may offset the amount of the overpayment against the final payment. In the event overpayment exceeds the final payment, CONTRACTOR shall pay COUNTY all such sums within five (5) business days of notice from COUNTY. Nothing herein shall be construed as limiting the remedies of COUNTY in the event an overpayment has been made.

19.4.5 Seventy-Five Percent Expenditure Notification:

19.4.5.1 CONTRACTOR shall maintain a system of record keeping that will allow CONTRACTOR to determine when it has incurred seventy-five percent (75%) of the total contract authorizations under this Agreement. Upon occurrence of this event, CONTRACTOR shall send written notification to ADMINISTRATOR.

20. OVERPAYMENTS

Any payment(s) made by COUNTY to CONTRACTOR in excess of that to which CONTRACTOR is entitled under this Agreement shall be repaid to COUNTY, in accordance with any applicable regulations and/or policies in effect during the term of this Agreement, or as established by COUNTY procedure. Any overpayments made by COUNTY which result from a payment by any other funding source shall be repaid, at the discretion of ADMINISTRATOR, to COUNTY or the funding source. Unless earlier repaid, CONTRACTOR shall make repayment within thirty (30) days after the date of the final audit findings report and prior

to any administrative appeal process. In the event an overpayment owing by CONTRACTOR is collected from COUNTY by the funding source, then CONTRACTOR shall reimburse COUNTY within thirty (30) days thereafter and prior to any administrative appeal process. CONTRACTOR agrees to pay all costs incurred by COUNTY necessary to enforce the provisions set forth in this Paragraph.

21. OUTSTANDING DEBT

CONTRACTOR shall have no outstanding debt with ADMINISTRATOR, or shall be in the process of resolving outstanding debt to ADMINISTRATOR's satisfaction, prior to entering into and during the term of this Agreement.

22. FINAL REPORT

CONTRACTOR shall complete and submit to ADMINISTRATOR a final report within sixty (60) days after the termination of this Agreement, which shall summarize the activities and services provided by CONTRACTOR during the term of this Agreement. CONTRACTOR and ADMINISTRATOR may mutually agree in writing to modify the date upon which the final report must be submitted.

23. INDEPENDENT AUDIT

23.1 CONTRACTOR shall employ a licensed certified public accountant who shall prepare and file with ADMINISTRATOR an annual organization-wide audit of related expenditures during the term of this Agreement in compliance with the 31 USC 7501 - 7507, as well as its implementing regulations under 2 CRF Part 200, Uniform Administrative Requirements, Cost Principles and Audit Requirements for Federal Awards. The audit must be performed in accordance with generally accepted government auditing standards and Title 2 CFR Part 230. CONTRACTOR shall cooperate with COUNTY, State and/or Federal agencies to ensure that corrective action is taken within six (6) months after issuance of all audit reports with regard to audit exceptions.

23.2 It is mutually understood that CONTRACTOR's yearly fiscal cycle covers October 1 through September 30. CONTRACTOR shall provide ADMINISTRATOR

copies of organization-wide audits for each of the fiscal cycles corresponding with the term of this Agreement. CONTRACTOR shall provide each audit within fourteen (14) calendar days of CONTRACTOR's receipt. Failure of CONTRACTOR to comply with this Paragraph shall be sufficient cause for ADMINISTRATOR to deny payment under this or any subsequent Agreement with CONTRACTOR until such time as the required audit(s) are provided to ADMINISTRATOR. ADMINISTRATOR may modify CONTRACTOR's audit submission deadline upon notice to CONTRACTOR.

24. RECORDS, INSPECTIONS AND AUDITS

24.1 Financial Records:

24.1.1 CONTRACTOR shall prepare and maintain accurate and complete financial records. Financial records shall be retained, by CONTRACTOR, for a minimum of five (5) years from the date of final payment under this Agreement or until all pending COUNTY, State and Federal audits are completed, whichever is later.

24.1.2 CONTRACTOR shall establish and maintain reasonable accounting, internal control and financial reporting standards in conformity with generally accepted accounting principles established by the American Institute of Certified Public Accountants and to the satisfaction of ADMINISTRATOR.

24.2 Client Records:

24.2.1 CONTRACTOR shall prepare and maintain accurate and complete records of CLIENTs served and dates and type of services provided under the terms of this Agreement in a form acceptable to ADMINISTRATOR.

24.2.2 CONTRACTOR shall keep all COUNTY data provided to CONTRACTOR during the term(s) of this Agreement for a minimum of five (5) years from the date of final payment under this Agreement or until all pending COUNTY, State and Federal audits are completed, whichever is later. These records shall be stored in Orange County, unless CONTRACTOR requests and

COUNTY provides written approval for the right to store the records in another county. Notwithstanding anything to the contrary, upon termination of this Agreement, CONTRACTOR shall relinquish control with respect to COUNTY data to COUNTY in accordance with Subparagraph 42.2.

24.2.3 Medical records pertaining to the Refugee Health Assessment Program (RHAP) shall be retained for a minimum of seven years, except for minors whose records shall be kept at least until one year after the minor has reached the age of 18, but in no case less than seven years, as per California Code of regulations, Title 22, Social Security, Division 5, Chapter 7, Article 6, Section 75055.

24.2.4 Contract Fiscal records/documents shall be maintained and made available to the State (upon request) for a period of three years from the date of final payment under the specific RHAP agreement.

24.2.5 COUNTY may refuse payment for a claim if CLIENT records are determined by COUNTY to be incomplete or inaccurate. In the event CLIENT records are determined to be incomplete or inaccurate after payment has been made, COUNTY may treat such payment as an overpayment within the provisions of this Agreement.

24.3 Public Records:

To the extent permissible under the law, all records, including but not limited to, reports, audits, notices, claims, statements and correspondence, required by this Agreement may be subject to public disclosure. COUNTY will not be liable for any such disclosure.

24.4 Inspections and Audits:

24.4.1 The U.S. Department of Health and Human Services, Comptroller General of the United States, Director of CDSS, State Auditor-General, ADMINISTRATOR, COUNTY's Auditor-Controller and Internal Audit Department, or any of their authorized representatives, shall have access to

any books, documents, papers and records, including medical records, of CONTRACTOR which any of them may determine to be pertinent to this Agreement for the purpose of financial monitoring. Further, all the above mentioned persons have the right at all reasonable times to inspect or otherwise evaluate the work performed or being performed under this Agreement and the premises in which it is being performed.

24.4.2 CONTRACTOR shall make its books and financial records available within the borders of Orange County within ten (10) days of receipt of written demand by ADMINISTRATOR.

24.4.3 In the event CONTRACTOR does not make available its books and financial records within the borders of Orange County, CONTRACTOR agrees to pay all necessary and reasonable expenses incurred by COUNTY, or COUNTY's designee, necessary to obtain CONTRACTOR's books and financial records.

24.4.4 CONTRACTOR shall pay to COUNTY the full amount of COUNTY's liability to the State or Federal government or any agency thereof resulting from any disallowances or other audit exceptions to the extent that such liability is attributable to CONTRACTOR's failure to perform under this Agreement.

24.5 Evaluation Studies:

24.5.1 CONTRACTOR shall participate as requested by COUNTY in research and/or evaluative studies designed to show the effectiveness and/or efficiency of CONTRACTOR's services or provide information about CONTRACTOR's project.

25. PERSONNEL DISCLOSURE

25.1 CONTRACTOR shall make available to ADMINISTRATOR a current list of all personnel providing services hereunder, including résumés and job applications. Changes to the list will be immediately provided to ADMINISTRATOR in writing, along with a copy of a résumé and/or job

application. The list shall include:

25.1.1 Names and dates of birth of all full or part-time personnel by title, including volunteer personnel, whose direct services are required to provide the programs described herein;

25.1.2 A brief description of the functions of each position and the hours each person works each week; or for part-time personnel, each day or month, as appropriate;

25.1.3 The professional degree, if applicable, and experience required for each position; and

25.1.4 The language skill, if applicable, for all personnel.

25.2 Where authorized by law, CONTRACTOR's employment applications shall require applicants to provide detailed information regarding the conviction of a crime by any court, for offenses other than minor traffic offenses. Information not disclosed in the employment application discovered subsequent to the hiring or promotion of any applicant shall be cause for termination of that employee from the performance of services under this Agreement.

25.3 Where authorized by law, CONTRACTOR shall conduct, at no cost to COUNTY, a clearance on the following public websites the names and dates of birth for all employees and/or volunteers who will have direct, interactive contact with CLIENTs served through this Agreement: U.S. Department of Justice National Sex Offender Website (www.nsopw.gov) and Megan's Law Sex Offender Registry (www.meganslaw.ca.gov).

25.4 Where authorized by law, CONTRACTOR shall conduct, at no cost to COUNTY, a criminal record background check on all employees (direct service and administrative) funded through this Agreement and also all non-funded staff (e.g., volunteers, in-kind staff, etc.) who will have direct, interactive contact with CLIENTs served through this Agreement. Background

checks conducted through the California Department of Justice shall include a check of the California Central Child Abuse Index, when applicable. Candidates will satisfy background checks consistent with this paragraph and their performance of services under this Agreement.

25.5 In the event a record is revealed through the processes described in Subparagraphs 25.3 and 25.4, COUNTY will be available to consult with CONTRACTOR on appropriateness of personnel providing services through this Agreement.

25.6 CONTRACTOR warrants that all persons employed or otherwise assigned by CONTRACTOR to provide services under this Agreement have satisfactory past work records and/or reference checks indicating their ability to perform the required duties and accept the kind of responsibility anticipated under this Agreement. CONTRACTOR shall maintain records of background investigations and reference checks undertaken and coordinated by CONTRACTOR for each employee and/or volunteer assigned to provide services under this Agreement for a minimum of five (5) years from the date of final payment under this Agreement or until all pending COUNTY, State and Federal audits are completed, whichever is later, in compliance with all applicable laws.

25.7 CONTRACTOR shall immediately notify ADMINISTRATOR concerning the arrest and/or subsequent conviction, for offenses other than minor traffic offenses, of any paid employee and/or volunteer staff performing services under this Agreement, when such information becomes known to CONTRACTOR. ADMINISTRATOR may determine whether such employee and/or volunteer may continue to provide services under this Agreement and shall provide notice of such determination to CONTRACTOR in writing. CONTRACTOR's failure to comply with ADMINISTRATOR's decision shall be deemed a material breach of this Agreement, pursuant to Paragraph 18 above.

25.8 COUNTY has the right to approve or disapprove all of CONTRACTOR's staff performing work hereunder and any proposed changes in CONTRACTOR's staff.

25.9 COUNTY shall have the right to require CONTRACTOR to remove any employee from the performance of services under this Agreement. At the request of COUNTY, CONTRACTOR shall immediately replace said personnel.

25.10 CONTRACTOR shall notify COUNTY immediately when staff is terminated for cause from working on this Agreement.

25.11 Disqualification, if any, of CONTRACTOR staff, pursuant to Paragraph 25, shall not relieve CONTRACTOR of its obligation to complete all work in accordance with the terms and conditions of this Agreement.

26. EMPLOYMENT ELIGIBILITY VERIFICATION

As applicable, CONTRACTOR warrants that it fully complies with all Federal and State statutes and regulations regarding the employment of aliens and others, and that all its employees performing work under this Agreement meet the citizenship or alien status requirement set forth in Federal statutes and regulations. CONTRACTOR shall obtain, from all employees performing work hereunder, all verification and other documentation of employment eligibility status required by Federal or State statutes and regulations including, but not limited to, the Immigration Reform and Control Act of 1986, Title 8 USC Section 1324 et seq., as they currently exist and as they may be hereafter amended. CONTRACTOR shall retain all such documentation for all covered employees for the period prescribed by the law. CONTRACTOR shall indemnify, defend with counsel approved in writing by COUNTY, and hold harmless, COUNTY, its agents, officers and employees from employer sanctions and any other liability which may be assessed against CONTRACTOR or COUNTY or both in connection with any alleged violation of any Federal or State statutes or regulations pertaining to the eligibility for employment of any persons

performing work under this Agreement.

27. ENFORCEMENT OF CHILD SUPPORT OBLIGATIONS

27.1 In order to comply with child support enforcement requirements of COUNTY, CONTRACTOR agrees to furnish to ADMINISTRATOR within thirty (30) days of the award of this Agreement:

(a) in the case of an individual contractor, his/her name, date of birth, Social Security number and residence address;

(b) in the case of a contractor doing business in a form other than as an individual, the name, date of birth, Social Security number and residence address of each individual who owns an interest of ten percent (10%) or more in the contracting entity;

(c) a certification that CONTRACTOR has fully complied with all applicable Federal and State reporting requirements regarding its employees; and

(d) a certification that CONTRACTOR has fully complied with all lawfully served Wage and Earnings Assignment Orders and Notices of Assignment, and will continue to so comply.

27.2 The failure of CONTRACTOR to timely submit the data or certifications required by subsections (a), (b), (c), or (d), or to comply with all Federal and State employee reporting requirements for child support enforcement or to comply with all lawfully served Wage and Earnings Assignment Orders and Notices of Assignment shall constitute a material breach of this Agreement, and failure to cure such breach within sixty (60) calendar days of notice from COUNTY shall constitute grounds for termination of this Agreement.

27.3 It is expressly understood that this data will be transmitted to governmental agencies charged with the establishment and enforcement of child support orders, and for no other purpose.

///

28. CHILD AND DEPENDENT ADULT/ELDER ABUSE REPORTING

CONTRACTOR shall establish a procedure acceptable to ADMINISTRATOR to ensure that all employees, volunteers, consultants or agents performing services under this Agreement report child abuse or neglect to one of the agencies specified in Penal Code Section 11165.9 and dependent adult or elder abuse as defined in Section 15610.07 of the WIC to one of the agencies specified in WIC Section 15630. CONTRACTOR shall require such employee, volunteer, consultant or agent to sign a statement acknowledging the child abuse reporting requirements set forth in Sections 11166 and 11166.05 of the Penal Code and the dependent adult and elder abuse reporting requirements as set forth in Section 15630 of the WIC and will comply with the provisions of these code sections as they now exist or as they may hereafter be amended.

29. NOTICE TO EMPLOYEES REGARDING THE SAFELY SURRENDERED BABY LAW

CONTRACTOR shall notify and provide to its employees, a fact sheet regarding the Safely Surrendered Baby Law, its implementation in Orange County and where and how to safely surrender a baby. The fact sheet is available on the Internet at www.babysafe.ca.gov for printing purposes. The information shall be posted in all reception areas where CLIENTs are served.

30. CONFIDENTIALITY

30.1 CONTRACTOR agrees to maintain the confidentiality of its records pursuant to WIC Sections 827 and 10850-10853, the CDSS MPP, Division 19-000, and all other provisions of law, and regulations promulgated thereunder relating to privacy and confidentiality, as each may now exist or be hereafter amended.

30.2 All records and information concerning any and all persons referred to CONTRACTOR by COUNTY or COUNTY's designee shall be considered and kept confidential by CONTRACTOR and CONTRACTOR's employees, volunteers, agents, and subcontractors. CONTRACTOR shall require all of its employees,

volunteers, agents, subcontractors and partners who may provide services for CONTRACTOR under this Agreement to sign an agreement with CONTRACTOR before commencing the provision of any such services, to maintain the confidentiality of any and all materials and information with which they may come into contact, or the identities or any identifying characteristics or information with respect to any and all participants referred to CONTRACTOR by COUNTY, except as may be required to provide services under this Agreement or to those specified in this Agreement as having the capacity to audit CONTRACTOR, and as to the latter, only during such audit. CONTRACTOR shall comply with any audits specified in Paragraph 24, provide reports and any other information required by COUNTY in the administration of this Agreement, and as otherwise permitted by law.

30.3 CONTRACTOR shall inform all of its employees, volunteers, agents, subcontractors and partners of this provision and that any person violating the provisions of said California state law may be guilty of a crime.

30.4 CONTRACTOR agrees that any and all subcontracts entered into shall be subject to the confidentiality requirements of this Agreement.

31. COPYRIGHT ACCESS

The U.S. Department of Health and Human Services, the CDSS, and COUNTY will have a royalty-free, nonexclusive and irrevocable license to publish, translate, or use, now and hereafter, all material developed under this Agreement including those covered by copyright

32. WAIVER

No delay or omission by either party hereto to exercise any right or power accruing upon any noncompliance or default by the other party with respect to any of the terms of this Agreement shall impair any such right or power or be construed to be a waiver thereof. A waiver by either of the parties hereto of any of the covenants, conditions, or agreements to be

performed by the other shall not be construed to be a waiver of any succeeding breach thereof or of any other covenant, condition or agreement herein contained.

33. PETTY CASH

CONTRACTOR is authorized to establish a petty cash fund in an amount not to exceed one thousand dollars ($1,000).

34. PUBLICITY

34.1 Information and solicitations, prepared and released by CONTRACTOR, concerning the services provided under this Agreement shall state that the program, wholly or in part, is funded through COUNTY, State and Federal government.

34.2 CONTRACTOR shall not disclose any details in connection with this Agreement to any person or entity except as may be otherwise provided hereunder or required by law. However, in recognizing CONTRACTOR's need to identify its services and related CLIENTs to sustain itself, COUNTY shall not inhibit CONTRACTOR from publishing its role under this Agreement within the following conditions:

34.2.1 CONTRACTOR shall develop all publicity material in a professional manner; and

34.2.2 During the term of this Agreement, CONTRACTOR shall not, and shall not authorize another to, publish or disseminate any commercial advertisements, press releases, feature articles, or other materials using the name of COUNTY without the prior written consent of COUNTY. COUNTY shall not unreasonably withhold written consent.

34.3 COUNTY owns all rights to the name, logos and symbols of COUNTY. The use and/or reproduction of COUNTY's name and/or logo for any purpose, including commercial advertisement, promotional purposes, announcements, displays or press releases, without COUNTY's prior written consent is

expressly prohibited.

35. COUNTY RESPONSIBILITIES

ADMINISTRATOR will provide consultation and technical assistance and will monitor performance of CONTRACTOR in meeting the terms of this Agreement.

36. REFERRALS

CONTRACTOR shall provide services to Clients referred by ADMINISTRATOR.

37. REPORTS

37.1 CONTRACTOR shall provide information deemed necessary by ADMINISTRATOR to complete any State-required reports related to the services provided under this Agreement.

37.2 CONTRACTOR shall maintain records and submit reports containing such data and information regarding the performance of CONTRACTOR's services, costs or other data relating to this Agreement, as may be requested by ADMINISTRATOR, upon a form approved by ADMINISTRATOR. ADMINISTRATOR may modify the provisions of this Paragraph upon written notice to CONTRACTOR.

38. ENERGY EFFICIENCY STANDARDS

As applicable, CONTRACTOR shall comply with the mandatory standards and policies relating to energy efficiency in the State Energy Conservation Plan (Title 24, CCR).

39. ENVIRONMENTAL PROTECTION STANDARDS

CONTRACTOR shall be in compliance with the Clean Air Act [Title 42 USC Section 7401 et seq.], the Clean Water Act (Title 33 USC Section 1251 et seq.), Executive Order 11738 and Environmental Protection Agency, hereinafter referred to as "EPA," regulations (Title 40 CFR), as any may now exist or be hereafter amended. Under these laws and regulations, CONTRACTOR assures that:

39.1 No facility to be utilized in the performance of the proposed grant has been listed on the EPA List of Violating Facilities;

39.2 It will notify COUNTY prior to award of the receipt of any

communication from the Director, Office of Federal Activities, U.S. EPA, indicating that a facility to be utilized for the grant is under consideration to be listed on the EPA List of Violating Facilities; and

39.3 It will notify COUNTY and EPA about any known violation of the above laws and regulations.

40. CERTIFICATION AND DISCLOSURE REGARDING PAYMENTS TO INFLUENCE CERTAIN FEDERAL TRANSACTIONS

CONTRACTOR shall be in compliance with Section 319 of Public Law 101-121 pursuant to Title 31 USC Section 1352 and the guidelines with respect to those provisions set down by the OMB and published in the Federal Register dated December 20, 1989, Volume 54, No. 243, pp. 52306-52332. Under these laws and regulations, it is mutually understood that any contract which utilizes Federal monies in excess of $100,000 must contain and CONTRACTOR must certify compliance utilizing a form provided by ADMINISTRATOR that cites the following:

A. The definitions and prohibitions contained in the clause at Federal Acquisition Regulation 52.203-12, Limitation on Payments to Influence Certain Federal Transactions, included in this solicitation, are hereby incorporated by reference in Paragraph (B) of this certification.

B. The offeror, by signing its offer, hereby certifies to the best of his or her knowledge and belief as of December 23, 1989, that

1) No Federal appropriated funds have been paid or will be paid to any person for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress on his or her behalf in connection with the awarding of any Federal contract, the making of any Federal grant, the making of any Federal loan, the entering into of any

cooperative agreement, and the extension, continuation, renewal, amendment or modification of any Federal contract, grant, loan or cooperative agreement;

2) If any funds other than Federal appropriated funds (including profit or fee received under a covered Federal transaction) have been paid, or will be paid, to any person for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress on his or her behalf in connection with this solicitation, the offeror shall complete and submit, with its offer, OMB standard form LLL, Disclosure of Lobbying Activities, to the Contracting Officer; and

3) He or she will include the language of this certification in all subcontract awards at any tier and require that all recipients of subcontract awards in excess of $100,000 shall certify and disclose accordingly.

C. Submission of this certification and disclosure is a prerequisite for making or entering into this Agreement imposed by Section 1352, Title 31, USC. Any person who makes an expenditure prohibited under this provision or who fails to file or amend the disclosure form to be filed or amended by this provision, shall be subject to a civil penalty of not less than $10,000, and not more than $100,000, for each such failure.

41. POLITICAL ACTIVITY

CONTRACTOR agrees that the funds provided herein shall not be used to promote or oppose, directly or indirectly, any political party, political candidate or political activity, except as permitted by law.

42. TERMINATION PROVISIONS

42.1 ADMINISTRATOR may terminate this Agreement without penalty immediately with cause or after thirty (30) days written notice without cause, unless otherwise specified. Notice shall be deemed served on the date of

mailing. Cause shall include but not be limited to any breach of contract, any partial misrepresentation whether negligent or willful, fraud on the part of CONTRACTOR, discontinuance of the services for reasons within CONTRACTOR's reasonable control, and repeated or continued violations of COUNTY ordinances unrelated to performance under this Agreement that in the reasonable opinion of COUNTY indicate a willful or reckless disregard for COUNTY laws and regulations. Exercise by ADMINISTRATOR of the right to terminate this Agreement shall relieve COUNTY of all further obligations under this Agreement.

42.2 For ninety (90) calendar days prior to the expiration date of this Agreement, or upon notice of termination of this Agreement ("Transition Period"), CONTRACTOR agrees to cooperate with ADMINISTRATOR in the orderly transfer of service responsibilities, active case records, and pertinent documents. The Transition Period may be modified as agreed upon in writing by the Parties. During the Transition Period, service and data access shall continue to be made available to COUNTY without alteration. CONTRACTOR also shall assist COUNTY in extracting and/or transitioning all data in the format determined by COUNTY.

42.3 In the event of termination of this Agreement, cessation of business by CONTRACTOR or any other event preventing CONTRACTOR from continuing to provide services, CONTRACTOR shall not withhold the COUNTY data or refuse for any reason, to promptly provide to COUNTY the COUNTY data if requested to do so on such media as reasonably requested by COUNTY, even if COUNTY is then or is alleged to be in breach of this Agreement.

42.4 The obligations of COUNTY under this Agreement are contingent upon the availability of Federal and/or State funds, as applicable, for the reimbursement of CONTRACTOR's expenditures, and inclusion of sufficient funds for the services hereunder in the budget approved by the Orange County Board

of Supervisors each fiscal year this Agreement remains in effect or operation. In the event that such funding is terminated or reduced, ADMINISTRATOR may immediately terminate this Agreement, reduce COUNTY's maximum obligation, or modify this Agreement, without penalty. The decision of ADMINISTRATOR will be binding on CONTRACTOR. ADMINISTRATOR will provide CONTRACTOR with written notification of such determination. CONTRACTOR shall immediately comply with ADMINISTRATOR's decision.

42.5 If any term, covenant, condition, or provision of this Agreement or the application thereof is held invalid, void, or unenforceable, the remainder of the provisions in this Agreement shall remain in full force and effect and shall in no way be affected, impaired, or invalidated thereby.

43. GOVERNING LAW AND VENUE

This Agreement has been negotiated and executed in the State of California and shall be governed by and construed under the laws of the State of California, without reference to conflict of law provisions. In the event of any legal action to enforce or interpret this Agreement, the sole and exclusive venue shall be a court of competent jurisdiction located in Orange County, California, and the parties hereto agree to and do hereby submit to the jurisdiction of such court, notwithstanding Code of Civil Procedure Section 394. Furthermore, the parties specifically agree to waive any and all rights to request that an action be transferred for trial to another county.

44. SIGNATURE IN COUNTERPARTS

The parties agree that separate copies of this Agreement may be signed by each of the parties, and this Agreement will have the same force and effect as if the original had been signed by all the parties.

CONTRACTOR represents and warrants that the person executing this Agreement on behalf of and for CONTRACTOR is an authorized agent who has actual authority to bind CONTRACTOR to each and every term, condition and

obligation of this Agreement and that all requirements of CONTRACTOR have been fulfilled to provide such actual authority.

///

///

///

///

///

///

///

///

///

///

///

///

///

///

///

///

///

///

///

///

///

///

///

///

WHEREFORE, the parties hereto have executed this Agreement in the County of Orange, California.

By: _____
KHOULOUD BUSTAMI
BOARD PRESIDENT
ACCESS CALIFORNIA SERVICES

Dated: 07/25/17

By: _____
CHAIRWOMAN
OF THE BOARD OF SUPERVISORS
COUNTY OF ORANGE, CALIFORNIA

Dated: _____

By: _____
MINZAH MALIK
BOARD SECRETARY
ACCESS CALIFORNIA SERVICES

Dated: 07/25/17

SIGNED AND CERTIFIED THAT A COPY OF THIS
AGREEMENT HAS BEEN DELIVERED TO THE CHAIR
OF THE BOARD PER G.C. SEC. 25103, RESO 79-1535
ATTEST:

_____
ROBIN STIELER
Clerk of the Board
Orange County, California

APPROVED AS TO FORM
COUNTY COUNSEL
COUNTY OF ORANGE, CALIFORNIA

By: _____
DEPUTY

Dated: 7/25/17

EXHIBIT A

TO

AGREEMENT

BETWEEN

COUNTY OF ORANGE

AND

ACCESS CALIFORNIA SERVICES

FOR THE PROVISION OF **REFUGEE SOCIAL SERVICES**

AND

REFUGEE HEALTH SERVICES

1. POPULATION TO BE SERVED

1.1 CONTRACTOR shall provide services to individuals who qualify as "Afghan or Iraqi alien granted Special Immigration Status (SIV) under section 101(a) (27) of the Immigration and Nationality Act (INA)," "Refugees," "Asylees," "Cuban and Haitian Entrants," "Amerasians," "Trafficking Victims," and "Parolees" as defined below. The population to be served will collectively be referred to as "CLIENTs."

1.1.1 Afghan or Iraqi alien granted Special Immigration Status (SIV) under section 101(a) (27) of the INA: Afghan and Iraqi Special Immigrants are displaced persons from Afghanistan and Iraq admitted to the U.S. with Special Immigrant Visas (SIVs). These Afghans and Iraqis were employed by or assisted the U.S. Armed Forces with translation and other services.

1.1.2 Amerasians: Persons born in Vietnam after January 1, 1962, and before January 1, 1976, and fathered by a U.S. citizen. The Amerasian's mother, her spouse, her other children or someone who has acted as the Amerasian's mother, father or next of kin (and the spouse and children of that person) are also included in this category. These CLIENTs are admitted

to the U.S. as immigrants pursuant to Section 584 of the Foreign Operations, Export Financing, and Related Programs Appropriations Act of 1988 as contained in Section 101(e) of Public Law 100-202 and amended by the 9th proviso under Migration and Refugee Assistance in Title II of the Foreign Operations, Export Financing, and Related Programs Appropriations Act of 1989 (Pub. L. No. 100-461 as amended).

1.1.3 Asylees: Persons as defined in the Immigration and Nationality Act (INA), 101 (1) (a) (42); 8 USC 1101 (a) (42) (a). An asylee is a person who travels on his/her own to the U.S., and applies for and is granted "asylum" status by the U.S. Citizenship and Immigration Services, which allows them to remain in the U.S. An asylee also meets the refugee definition as a person having no nationality, is outside of the country in which that person habitually resided, "and who is unable or unwilling to return to, and is unable or unwilling to avail himself or herself of the protection of, that country because of persecution or a well-founded fear of persecution on account of race, religion, nationality, membership in a particular social group, or political opinion." Asylees must be at least eighteen (18) years of age and not full-time students in primary or secondary school.

1.1.4 Cuban and Haitian Entrants: Defined under 45 CFR 401.2 as: (a) any individual granted parole status as a Cuban/Haitian Entrant (Status Pending) or granted any other special status subsequently established under the immigration laws for nationals of Cuba and Haiti, regardless of the status of the individual at the time assistance or services are provided; and (b) any other national of Cuba or Haiti (1) who: (i) was paroled in the U.S. and has not yet acquired any other status under the INA; (ii) is the subject of exclusion or deportation proceedings under the INA; or (iii) has an application for asylum pending with the U.S. Citizenship and Immigration

Services; and (2) with respect to whom a final, non-appealable, and legally enforceable order of deportation or exclusion has not been entered.

1.1.5 Refugees: Persons as defined in 8 USC 1101 (a) (42) (A). A refugee is a "person who is outside any country of such person's nationality or, in the case of a person having no nationality, is outside any country in which such persons habitually resided, and who is unable or unwilling to return to, and is unable or unwilling to avail himself or herself of the protection of, that country because of persecution or a well-founded fear of persecution on account of race, religion, nationality, membership of a particular social group, or political opinion." Refugees must be at least eighteen (18) years of age and not full-time students in primary or secondary schools.

1.1.6 Trafficking Victims: Adults who have been certified under the Trafficking Protection Act of 2000 by the Office of Refugee Settlement (ORR) as having experienced severe forms of trafficking. Severe forms of trafficking is defined as: (A) sex trafficking in which a commercial sex act is induced by force, fraud or coercion, (B) the recruitment, harboring, transportation, provision, or obtaining of a person for labor or services, through the use of force, fraud, or coercion for the purpose of subjection to involuntary servitude, peonage, debt bondage, or slavery. Family members accompanying/following to join victims of a severe form of trafficking, who have been granted nonimmigrant visas under 8 USC 1101(a)(15)(T)(ii), are eligible to the same benefits and services as refugees.

Trafficking and Crime Victims Assistance Program (TCVAP) eligible aided and non-aided individuals may receive Refugee Resettlement Program benefits and services to the same extent as refugees prior to receiving certification by ORR.

///

1.1.7 Individuals paroled as refugees under section 212(d) (5) under the Immigration and Nationality Act (INA): Paroled as a refugee is a category of parole, however, these individuals do not have refugee status and are not admitted to the United States in refugee status but rather parolees, and may receive Refugee Resettlement Program benefits and services to the same extent as refugees.

1.2 It is mutually understood that only CLIENTs who have resided in the United States (U.S.) for less than five (5) years are eligible to receive services under the Refugee Social Services (RSS) program, unless ADMINISTRATOR is granted a waiver by the Office of Refugee Resettlement (ORR), which will permit ADMINISTRATOR to serve CLIENTs who have not obtained citizenship, regardless of length of residency in the U.S.

2. PROGRAM GOALS

It is mutually understood that the primary objective of the RSS program is to foster the CLIENT's/Family's well-being by providing mentoring, employment, and supportive services that will assist with refugee resettlement. These services support CLIENTs in retaining employment and/or obtaining a higher paying job, thus assisting CLIENTs in moving towards self-sufficiency.

3. DEFINITIONS

3.1 CalWORKs: California Work Opportunity and Responsibility to Kids Act of 1997 as described in WIC, Section 11200 et seq.

3.2 Employment Support Services/Job Retention Services: Services provided to increase the likelihood of securing employment, retaining employment, and increasing income, thereby reducing assistance payments and recidivism, while promoting Family stability and economic self-sufficiency.

3.3 Employment Preparation Workshops (EPW): Provides techniques to enhance employability through group presentations and individual support in

coaching and development of interviewing skills, resume writing and application assistance, access to job leads, employer recruitments, and Job Fairs, one-on-one coaching, and employability assessments. Employment preparation shall include access to employment directed resources such as computers, copy and fax machines, telephones, computer training, and workplace acculturation training to address certain employment related social adjustment topics.

3.4 English Language Training (ELT): An instruction course, in English, for non-native English speakers with an emphasis on acquisition of survival and employment-related reading, writing, listening, and speaking skills.

3.5 Ethnic Community Based Organizations (ECBOs): Community based organizations established and operated by current or former refugees. The main focus of these organizations is to provide assistance to other refugees.

3.6 Family: CLIENT and his/her relatives living in the same household, or a married couple.

3.7 Family Self-Sufficiency Plan (FSSP): A plan that not only focuses on tangible barriers to employment but also incorporates other areas of potential need. The Plan addresses a CLIENT's/Family's need for employment-related services, as well as the need for other social services, and includes: (1) a determination of the total amount of income a particular Family would need to earn to exceed its Refugee Cash Assistance (RCA) and move into self-sufficiency without suffering a monetary penalty; (2) a strategy and timetable for obtaining that level of Family income through the placement in employment of sufficient numbers of employable Family members at sufficient wage levels; and, (3) employability plans for members of the same Family that are part of the Family Self-Sufficiency Plan.

3.8 Job Placement: The entry of CLIENTs into unsubsidized employment.

3.9 Job Ready: Individuals who possess the language skills to meet the minimum requirements to look for and accept employment, possess a Social Security number, and Employment Authorization Document (EAD) which is authorization to accept employment in the US.

3.10 Job Search Assistance: Services that provide the CLIENT with training to learn basic job seeking and interviewing skills, to understand employer expectations, and to learn skills designed to enhance an individual's capacity to move toward self-sufficiency.

3.11 Job Search: An activity in which the CLIENT's principal activity is to seek employment.

3.12 Mandatory Referrals: CLIENTs receiving RCA who are required to participate in an employment services program in order to continue to receive RCA.

3.13 Mandatory Work Registration and Sanctioning System: Requirements in the CDSS County Refugee Program Guidelines for RSS, used for determining eligibility for RCA, determining if a CLIENT must be considered a Mandatory Referral for Employment Services, explaining to a CLIENT his/her rights and responsibilities, and determining procedures when a CLIENT is not participating or not cooperating. The County Refugee Program Guidelines for RSS can be found at: http://www.cdss.ca.gov/refugeeprogram/res/pdf/CountyGuidelines/06Guidelines.pdf

3.14 On-the-Job-Training (OJT): Subsidized employment in which a CLIENT receives job skills training from an employer. At the end of the training it is expected that the CLIENT will be retained by the employer.

3.15 Other Employability Services: Employability assessment, child care, transportation, and interpretation/translation.

3.16 Part-Time Placement: RCA recipients working less than thirty-two

(32) hours per week.

3.17 Refugee Cash Assistance (RCA): An assistance program administered by state public welfare programs for newly arrived CLIENTs who do not meet the eligibility requirements for CalWORKs assistance or Supplemental Security Income (SSI).

3.18 Resettlement Agency (RA): A local community agency, which provides resettlement assistance and services to eligible CLIENTs.

3.19 Vocational English as a Second Language (VESL): English language instruction that provides the CLIENT with the language skills needed to seek, obtain, and maintain employment.

4. SERVICE DELIVERY MODEL

4.1 Program Objectives:

4.1.1 RSS is the process by which a Case Manager works directly with the CLIENT to assess the CLIENT's education, work experience and vocational skills, and subsequently determines the appropriate means for the CLIENT to obtain employment as quickly as possible. The Case Manager provides social work and employment related services to CLIENTs consistent with best practices that will assist CLIENTs in obtaining employment and address any barriers that may prevent them from achieving or maintaining economic self-sufficiency.

4.2 Principles:

CONTRACTOR shall:

4.2.1 Ensure services are conducted in a manner responsive to literacy, language, and socio-cultural issues that may impact CLIENTs/Families.

4.2.2 Be trained in cultural differences to ensure their ability to recognize and help CLIENTs who demonstrate language or cultural barriers to employment, including resistance to pursuing employment in

occupations that may be perceived as nontraditional;

4.2.3 Identify and be cognizant of the barriers related to domestic violence, mental health, and/or substance abuse issues, and provide services or make the appropriate referrals to address the barrier.

4.2.4 Ensure CLIENTs/Families are actively referred to needed services and follow-up to ensure the referral was successful;

4.2.5 Ensure opportunities are maximized to provide integrated, coordinated, and easily accessible resources for CLIENTs/Families;

4.2.6 Ensure services are community-based and provide integrated services that coordinate Federal, State, and community funding opportunities;

4.2.7 Identify CLIENT's strengths utilizing motivational and strength-based techniques; and

4.2.8 Ensure services are outcome-driven and identify indicators that accurately reflect progress towards outcomes identified in Subparagraph 5 of this Exhibit A.

4.3 Hours of Operation

4.3.1 CONTRACTOR shall provide service hours that are responsive to the needs of the target population(s) as determined by ADMINISTRATOR. At a minimum, CONTRACTOR must provide services Monday through Friday, from 8:00 a.m. to 5:00 p.m., except COUNTY holidays as established by the Orange County Board of Supervisors. However, CONTRACTOR is encouraged to provide the contracted services on holidays, whenever possible.

4.3.2 CONTRACTOR's holiday schedule shall not exceed COUNTY's holiday schedule which is as follows: New Year's Day, Martin Luther King Day, President Lincoln's Birthday, Presidents' Day, Memorial Day, Independence Day, Labor Day, Columbus Day, Veterans Day, Thanksgiving Day, Friday after Thanksgiving, and Christmas Day. CONTRACTOR shall obtain prior written

approval from ADMINISTRATOR for any closure outside of COUNTY's holiday schedule or the hours in Subparagraph 4.3.1. Any unauthorized closure shall be deemed a material breach of this Agreement, pursuant to Paragraph 18, and shall not be reimbursed.

5. PERFORMANCE REQUIREMENTS

CONTRACTOR shall meet, but shall not be limited to, the following outcomes during the term of this Agreement:

5.1 For the period of October 1, 2017 through September 30, 2018:

5.1.1 A minimum of forty percent (40%) of all unduplicated CLIENTs (aided and non-cash aided) identified in Subparagraph 6.1.1 are placed in either full time or part time employment.

5.1.2 A minimum of sixty percent (60%) of all unduplicated Job Ready CLIENTs (aided and non-cash aided) identified in Subparagraph 6.1.1 are placed in either full time or part time employment.

5.1.3 A minimum of eighty-five percent (85%) of the unduplicated CLIENTs identified in Subparagraph 5.1.1 and 5.1.2 retain employment for ninety (90) days.

5.1.4 A minimum of twenty percent (20%) of the total unduplicated CLIENTs identified in Subparagraph 5.1.1 and 5.1.2 obtain an average wage of at least eighteen percent (18%) above the prevailing California minimum wage.

5.2 For the period of October 1, 2018 through September 30, 2019:

5.2.1 A minimum of forty-five percent (45%) of the all unduplicated CLIENTs (aided and non-cash aided) identified in Subparagraph 6.1.1 are placed in either full time or part time employment.

5.2.2 A minimum of sixty-five percent (65%) of all unduplicated Job Ready CLIENTs (aided and non-cash aided) identified in Subparagraph 6.1.1 are placed in either full time or part time employment.

5.2.3 A minimum of eighty-five percent (85%) of the unduplicated CLIENTs identified in Subparagraph 5.2.1 and 5.2.2 retain employment for ninety (90) days.

5.2.4 A minimum of twenty percent (20%) of the total unduplicated CLIENTs identified in Subparagraph 5.2.1 and 5.2.2 obtain an average wage of at least eighteen percent (18%) above the prevailing California minimum wage.

5.3 For the period of October 1, 2019 through September 30, 2020:

5.3.1 A minimum of fifty percent (50%) of the all unduplicated CLIENTs (aided and non-cash aided) identified in Subparagraph 6.1.1 are placed in either full time or part time employment.

5.3.2 A minimum of seventy percent (70%) of all unduplicated Job Ready CLIENTs (aided and non-cash aided) identified in Subparagraph 6.1.1 are placed in either full time or part time employment.

5.3.3 A minimum of eighty-five percent (85%) of the unduplicated CLIENTs identified in Subparagraph 5.3.1 and 5.3.2 retain employment for ninety (90) days.

5.3.4 A minimum of twenty percent (20%) of the total unduplicated CLIENTs identified in Subparagraph 5.3.1 and 5.3.2 obtain an average wage of at least eighteen percent (18%) above the prevailing California minimum wage.

5.4 ADMINISTRATOR, in its sole discretion, may require changes to the outcome objectives stated above, to comply with any changes in law, or State or Federal regulations.

6. SERVICES TO BE PROVIDED

6.1 Employment Services

6.1.1 CLIENTs to be served will be non-cash and cash aided CLIENTs who have been in the U.S. for sixty (60) months or less. Pursuant to

45 CFR Part 400.147, priority for participation in services is as follows: 1) refugees during their first year in the U.S., 2) refugees receiving cash assistance, 3) unemployed refugees who are not receiving cash assistance, and 4) employed refugees who are in need of services to retain employment or attain economic independence. Cash aided CLIENTs are those CLIENTs in the Refugee Cash Assistance (RCA) Program. Those eligible for RCA are needy refugees without eligible minor children, who are not otherwise eligible for any other cash aid. CLIENTs may be eligible for 8 months of RCA. Mandatory Referrals must participate in refugee specific employment services and are eligible to receive other social services during the same 8-month period. These may include employability services, multi-leveled English language instruction, transportation, citizenship and employment authorization document assistance, translation/interpretation services, when necessary in connection with employment or participation in an employability service, and other services. The following description of Employment Services is applicable to RCA and the non-cash aided populations.

6.1.2 Intake and Assessment

CONTRACTOR shall:

6.1.2.1 Accept and provide Employment Services to all CLIENTs referred by ADMINISTRATOR.

6.1.2.2 Serve non-cash aided CLIENTs referred from public and private agencies, and self-referrals, if there are openings after all CLIENTs referred by ADMINISTRATOR have been served.

6.1.2.3 Verify eligibility of CLIENTs for services by viewing and photocopying, as appropriate, resident alien cards, U.S. Citizenship and Immigration Services I-94 forms, asylum approval letters, trafficking victim Federal certification letters, T(i) or T(ii) visas, drivers' licenses, and proof of residence in Orange County.

6.1.2.4 Provide registration verification, certification, and complete the necessary forms as required by ADMINISTRATOR.

6.1.2.5 Explain the Mandatory Work Registration and Sanctioning process to cash aided CLIENTs.

6.1.2.6 Administer an ADMINISTRATOR approved version of the Basic English Skills Test (BEST), an assessment that tests for reading and writing skills, to determine the individual's Student Performance Level (SPL).

6.1.2.7 Ensure that a cash aided CLIENT with a SPL lower than four (4) is enrolled in VESL classes and also assigned to EPW and Job Counseling as described in Subparagraphs 6.1.3 and 6.1.4 below, in accordance with the FSSP. A CLIENT with a SPL of four (4) shall be referred, as determined appropriate by CONTRACTOR, to VESL or the full range of Employment Services as described in this Paragraph 6. A CLIENT with a SPL level of five (5) or higher shall be referred for the full range of Employment Services, excluding VESL. All CLIENTs with a SPL of five (5) or higher shall immediately start Job Search while attending EPW.

6.1.2.8 Assign a Case Manager to each CLIENT to assess his/her potential to obtain employment and develop a FSSP. To the degree possible, CONTRACTOR shall assign all members of a Family to one Case Manager.

6.1.2.9 Conduct an orientation of the program requirements for all CLIENTs in their native languages whenever possible and if not, in languages that CLIENTs understand, explaining public assistance (to cash aided CLIENTs), the established grievance procedures, the purpose of the refugee programs, the training and Employment Services available, and the employment focus and goal of these programs.

6.1.2.10 Obtain information including, but not limited

to, personal data, health status, work history, educational background, language proficiency, job skills, previous training received, length of time in the U.S., and barriers, if any, to training and employment.

6.1.2.11 Provide an inclusive assessment of the Family to design a comprehensive service strategy that not only focuses on tangible barriers to employment but also incorporates other areas of potential need. This strategy will form the basis of the FSSP that addresses the Family's needs from the time of arrival until the attainment of economic independence. The FSSP should address the CLIENT's and/or Family's need for employment-related services as well as the need for other social services.

6.1.2.12 Develop individual employability plans for each CLIENT and/or Family member.

6.1.2.13 Enroll all eligible CLIENTs into Employment Services.

6.1.2.14 Encourage non-cash aided CLIENTs to follow the same service flow, if possible. However, since non-cash aided CLIENTs participate voluntarily, CLIENTs may opt to attend EPW, instead of following the service flow, prior to Job Placement.

6.1.2.15 Determine which of the services outlined in Paragraph 6 of this Exhibit A, or other available services the CLIENT/Family needs that support the FSSP, and include these services in the FSSP.

6.1.2.16 Assess Employment Support Services needs such as, but not limited to, acculturation, household budgeting, housing, and nutritional concerns.

6.1.3 EPW, Resources, and Transportation

CONTRACTOR shall:

6.1.3.1 Provide multi-leveled EPW, a minimum of once a week for CLIENTs. Topics of workshops shall have prior approval by

ADMINISTRATOR.

6.1.3.2 Include additional workshop sessions to address certain employment related social adjustment topics such as different cultures in American society, cultural conflicts at the work place, housing, health care, legal services, vocational training, work safety, and employee's rights. To promote self-sufficiency, CONTRACTOR shall utilize guest speakers during the workshops to present best practices and experiences in the employment services process. Guest speakers shall be from ECBOs and Community-Based Organizations (CBO), and former CLIENTs.

6.1.3.3 Establish access to resources for CLIENTs to practice skills learned in EPW. Resources shall include, but not be limited to, telephones, directories, newspapers, DVDs, videotapes, personal computers, recorders, and other tools to facilitate activities in practicing skills learned in EPW.

6.1.3.4 Provide transportation to interviews and job fairs, accompany CLIENTS to oversee completion of employment applications, and assist with translation during interviews as needed.

6.1.4 Job Counseling and Job Search Assistance

CONTRACTOR shall provide Job Counseling and Job Search Assistance concurrently to CLIENTs working Part-Time. CLIENTS receiving Job Counseling and Job Search Assistance may also be enrolled in vocational training.

CONTRACTOR shall:

6.1.4.1 Ensure CLIENTs employed less than thirty-two (32) hours per week are participating in additional Employment Services activities, in accordance with Subparagraphs 6.1 of this Exhibit A, provided that such services do not interfere with the CLIENT's job.

6.1.4.2 Maintain weekly contacts with CLIENTs in

order to monitor Job Search efforts/outcomes.

6.1.4.3 Identify and address barriers to employment and monitor progress on a weekly basis.

6.1.4.4 Conduct weekly individualized support sessions to build CLIENT's confidence in applying and interviewing for jobs and discuss job search activities and experiences, to offer tips, and to provide new strategies for approaching potential employers.

6.1.4.5 Provide personalized Job Search Assistance and Job Retention Services with orientation and awareness of the local job market and direction in locating job opportunities.

6.1.4.6 Provide Job Counseling to assist partially or temporarily employed CLIENTs to upgrade to full-time employment.

6.1.4.7 Provide job leads to increase skills and/or earnings.

6.1.4.8 Develop a Job Search Assistance plan that requires CLIENTs to file a minimum of five (5) job applications per week with potential employers, and conduct a minimum of one (1) contact with CONTRACTOR per week. CLIENTs enrolled in VESL are exempt from the requirement of filing a minimum of five (5) job applications per week until they begin their fifth (5^{th}) month in the U.S. VESL CLIENTs can be provided job leads per Subparagraph 6.1.4.7 if their job and language skills meet the minimum requirements for the required job duties.

6.1.5 Short-Term Skills Training (ST)

CONTRACTOR shall:

6.1.5.1 Evaluate and refer CLIENTs for ST offered by providers such as adult education centers, regional occupational programs, and community colleges.

6.1.5.2 Monitor CLIENTs attendance in training

programs not provided by CONTRACTOR, including obtaining attendance records; and identify and address barriers to program completion.

6.1.5.3 Document attendance and ensure ST programs do not exceed four (4) months.

6.1.6 Job Development and Placement

CONTRACTOR shall:

6.1.6.1 Provide CLIENTs with job leads and information regarding potential employers and prepare CLIENTs for job application completion and job interviews, including providing CLIENTs with clear expectations of potential job duties, and hours of employment to enhance successful job placement.

6.1.6.2 Provide individualized services to CLIENTs at the Resource Center as described in Subparagraph 7.2 of this Exhibit A.

6.1.6.3 Secure and/or provide any necessary transportation to potential employment sites and interviews, exploring employer-sponsored car pools, placing Family members in staggered shifts to alleviate transportation issues, and developing jobs accessible by public transportation.

6.1.6.4 Serve as a liaison and support between CLIENTs and employers.

6.1.6.5 Monitor CLIENTs during probationary period of employment, assess compatibility with employer, and problem solve as needed.

6.1.7 Employment Support, Job Retention Services, and Other Employability Services

CONTRACTOR shall provide the following Employment Support, Job Retention, and Other Employability Services for a period of up to twelve (12) months from employment date or until the termination of CONTRACTOR's agreement with ADMINISTRATOR, whichever occurs first:

6.1.7.1 Individualized or group vocational counseling offered during regular business and non-business hours to meet the needs of employed CLIENTs and to assist them to retain employment, or to increase earning capacity by identifying opportunities for advancement, learning new skills, upgrading present skills, finding better paying jobs, replacing lost jobs, and helping Part-Time employed CLIENTs to secure full-time positions.

6.1.7.2 Services that address issues and barriers to attaining self-sufficiency that may range from referral for resolution of behavioral health issues to facilitation of emergency services and access to available community resources.

6.1.7.3 Ongoing support and translation services to CLIENT and employer to resolve problems that CLIENTs may face at the work place such as conflicts with co-workers of different ethnic groups and maximize the effectiveness of the placement and help to maintain a positive image within the local labor market.

6.1.7.4 Follow-up by contacting with employed CLIENTs after the first week to determine their job satisfaction, to identify and help solve problems, and to generally provide further employment counseling.

6.1.7.5 Follow-up by contacting the CLIENT/Family after placement to determine retention and assess the CLIENT's/Family's progress towards the goal of self-sufficiency within the following:

6.1.7.5.1 Conduct a follow-up by contacting the CLIENT(s)/family thirty (30) and sixty (60) calendar days after placement to assess the individual's/family's progress toward the goal of self-sufficiency. Should a CLIENT loses his/her job, provide supportive counseling to prevent the CLIENT from experiencing a sense of failure and to encourage efforts to seek employment again.

6.1.7.5.2 Contact the employers and/or CLIENT(s)/family ninety (90) calendar days after placement to determine retention and assess the individual's/family's progress toward the goal of self-sufficiency.

6.1.7.5.3 After six months (180 days) of employment, the Employment Counselor will contact employers as well as the employee to ensure the CLIENT(s) is making satisfactory progress in the job. The Employment Counselor will then complete and close the CLIENT's file, the placement will have been successful and report to SSA.

6.1.7.6 Retain an active CLIENT file for a period of twelve (12) months from employment or until the termination of this Agreement, whichever occurs first.

6.1.7.7 Refer CLIENTs for English Language Training (ELT) and/or Skills Training classes conducted by local educational providers or CONTRACTOR(s) to promote continued education, and to assist the CLIENT in learning new skills or enhance present job skills to increase earnings potential.

6.1.8 Vocational English as a Second Language Services (VESL)

CONTRACTOR shall:

6.1.8.1 Enroll CLIENTs in VESL for a maximum of three (3) months.

6.1.8.2 Document attendance in accordance with Subparagraph 8.4 of this Exhibit A.

6.1.8.3 Provide classroom training of the English language as it relates to finding, obtaining, and maintaining employment. CLIENTs may be temporarily excused from classes for job interviews when and if appropriate job openings are identified.

6.1.8.4 Utilize a curriculum that is ELT correlated

with emphasis on job-related terminology.

6.1.8.5 Provide instruction for a minimum of fifteen (15) hours per week. Class instruction will be offered during business hours of Monday through Friday, 8:00 a.m. to 5:00 p.m., with instructional offerings during non-business hours to meet the needs of the target population.

6.1.8.6 Provide different levels of VESL, as appropriate, to meet CLIENT's needs.

6.1.8.7 Integrate monthly workshops, preferably employment related, with VESL classes; workshops and materials must be pre-approved by ADMINISTRATOR.

6.1.8.8 Work with school districts and community colleges to secure in-kind contributions of classroom space and/or teachers. If community colleges and school district teachers contribute to less than fifteen (15) hours of instruction per week, CONTRACTOR will mobilize community and CONTRACTOR staff supports to supplement the teachers during the uncovered hours.

6.1.8.9 Conduct post testing on all enrollees tested per Subparagraph 6.1.2.6 of this Exhibit A, to document individual progress as well as success of the instruction, and record test results in the CLIENT's file.

6.2 Outreach and Referral to Low Income Programs:

CLIENTs to be served shall be both cash aided and non-cash aided CLIENTs, who are not Employment Services participants.

6.2.1 Intake and Assessment

CONTRACTOR shall:

6.2.1.1 Accept all referrals from SSA, public and private agencies, and self-referrals for CLIENTs.

6.2.1.2 Accept cash aided and non-cash aided CLIENTs.

6.2.1.3 Solicit eligible CLIENTs on a voluntary basis.

6.2.1.4 Verify eligibility for services by viewing and photocopying, as appropriate, resident alien cards, U.S. Citizenship and Immigration Services' I-94 forms, asylum approval letters, trafficking victim Federal certification letters, T(i) or T(ii) visas, driver's licenses, and proof of residence in Orange County.

6.2.1.5 Provide registration verification, and complete the necessary forms as required by ADMINISTRATOR.

6.2.1.6 Assign a Case Manager to each CLIENT who shall act as an advisor to assess the CLIENT's/Family's needs, and who will inform them of community resources, make appropriate referrals, and follow-up.

6.2.1.7 Refer CLIENTs to Low Income Programs, as described in Subparagraph 6.2.3.1 of this Exhibit A, and follow up to confirm outcome of referral. Make any additional referrals for services as needed.

6.2.1.8 Conduct an orientation on the purpose and goals of the RSS program as described in Subparagraph 2 of this Exhibit A, the available services as described in Paragraph 6 of this Exhibit A, and the Formal Grievance Process as described in Subparagraph 9.7 of this Exhibit A for all CLIENTs in their native language whenever possible, and if not, in a language that the CLIENT understands.

6.2.1.9 Conduct a service needs assessment, documenting on a form approved by ADMINISTRATOR, at a minimum, the issues and barriers to attaining and maintaining stability, community integration and self-sufficiency, and the services required to address the CLIENT's/Family's needs which will improve the CLIENT's/Family's quality of life. For CLIENTs participating in Employment Services, this strategy shall be included as part of the FSSP.

6.2.2 Outreach

CONTRACTOR shall conduct on-going activities to identify and notify CLIENTs/Families of available services, service locations, and how to access the services provided under this Agreement.

6.2.3 Referral to Low Income Programs

CONTRACTOR shall:

6.2.3.1 Refer CLIENTs/Families for other appropriate services or community resources including, but not limited to, Head Start; Women, Infants, and Children's Services Program (WIC); Cal Fresh; Covered California; Medi-Cal; Low Income Home Energy Assistance Program (LIHEAP); the Utility Company's Reduced Rate Programs (RRP); consumer education programs; childcare services and payment programs; low income housing assistance and housing subsidy programs, including first time buyer programs; food assistance programs such as food banks, RAs, and ECBOs; and other local community agencies providing services, as appropriate, to remove barriers and/or improve the CLIENT's/Family's quality of life by increasing access to services.

6.2.3.2 Refer non-cash aided CLIENTs/Families to SSA, the Social Security Administration, or other agencies providing financial assistance as appropriate.

6.2.3.3 Provide CLIENTs/Families with community resource materials.

6.2.3.4 Provide CLIENTs/Families assistance in enrolling in low income programs by making application forms available and assisting in completion of the forms.

6.2.3.5 Follow-up with CLIENTs/Families to ensure referrals to services outside CONTRACTOR's agency were successful.

6.3 Interpretation/Translation Services

CONTRACTOR shall:

6.3.1 Provide CLIENTs/Families interpretation/translation services to assist with enrollment in low-income programs, or make the appropriate referral.

6.3.2 Provide CLIENTs/Families legal or medical interpretation/translation services, or make the appropriate referral.

6.3.3 Follow-up with CLIENTs referred to services outside the CONTRACTOR's agency.

6.4 Mentoring Services

CLIENTs and their families are eligible to receive Mentoring Services if they are eligible to receive RSS pursuant to this Agreement and if they have been residing in the U.S. for less than one year.

CONTRACTOR shall:

6.4.1 Develop a plan that addresses the CLIENT's/Family's concerns; the need for acculturation and specialized needs; and the need for other social services, such as, but not limited to, Medi-Cal and Cal Fresh. For CLIENTs participating in Employment Services, this strategy should be included as part of the FSSP.

6.4.2 Refer CLIENT's/Families as needed to RAs, ECBOs, other service agencies, or other COUNTY contracted service providers, as appropriate, to assist CLIENT's/Families to address barriers including, but not limited to, personal health, Family conflict, housing, and transportation issues.

6.5 Older Refugees

6.5.1 Citizenship and Naturalization Services

Older Refugees, including Asylees, SIVs, and Cuban and Haitian Entrants, are eligible to receive or be referred to Citizenship and Naturalization Services. Older Refugees are defined as Refugees sixty (60) years of age and over. CONTRACTOR shall provide services in order to

facilitate self-sufficiency:

6.5.2 Outreach, Education, and Translation

6.5.2.1 CONTRACTOR shall conduct outreach, and provide education to older refugees on available services and how to obtain these services

6.5.2.2 CONTRACTOR shall provide translation and interpretation services to older refugees.

6.5.3 Linkages

6.5.3.1 CONTRACTOR will establish linkages with local Area Agencies on Aging, to enhance awareness in order to make mainstream senior programs more linguistically and culturally appropriate to older refugees.

6.5.4 English Language Training (ELT)

6.5.4.1 CONTRACTOR shall provide or refer Older Refugees to ELT specifically designed for Older Refugees who are preparing for naturalization.

6.5.5 Citizenship Training

CONTRACTOR shall:

6.5.5.1 Provide or refer Older Refugees to citizenship classes with a curriculum consisting of integrated instruction in American history and civics. Lessons will include preparation for the U.S. Citizenship and Immigration Services interview.

6.5.5.2 Provide training for Older Refugees with an understanding of their basic rights and responsibilities as U.S. citizens.

6.5.6 Naturalization Application Assistance

CONTRACTOR shall:

6.5.6.1 Provide application assistance to facilitate Older Refugees in completing the application process, including appointments

to take the written civics and history exams.

6.5.7 Transportation

CONTRACTOR shall:

6.5.7.1 Provide transportation to Older Refugees in need of transportation services to classes and citizenship naturalization services.

6.5.7.2 Maintain a log of the CLIENTs that receive this service.

7. OTHER CONTRACTOR REQUIREMENTS

CONTRACTOR shall:

7.1 Follow ADMINISTRATOR's and California Department of Social Services' current procedures concerning any CLIENT's failure to participate or cooperate. ADMINISTRATOR will forward such procedures to CONTRACTOR.

7.2 Offer an onsite Resource Center that includes, but shall not be limited to, the following:

7.2.1 Computer labs;

7.2.2 Audio/visual training equipment;

7.2.3 Resume preparation assistance;

7.2.4 Job Search;

7.2.5 Internet access;

7.2.6 Phone banks;

7.2.7 Resource directories;

7.2.8 Local Newspapers; and

7.2.9 Fully staffed during normal business hours, and additional hours as needed.

7.3 Utilize the Family Self-Sufficiency Plan (FSSP) to monitor the CLIENT's progress through the RSS program and through other service providers. Monitoring includes, but is not limited to, Job Placement, employment

retention, status of referrals to service providers and changes to an individual's personal data. This will also include completing all Mandatory Referral forms as well as coordinating with and providing information, as determined necessary by ADMINISTRATOR, to the referring agencies.

7.4 Document progress, attendance and participation hours in accordance with Subparagraph 8.4 of this Exhibit A.

7.5 Document failure by a cash aided CLIENT to participate/cooperate utilizing forms provided by ADMINISTRATOR.

7.6 Forward to ADMINISTRATOR appropriate documentation of noncompliance and nonparticipation regarding a CLIENT who is required to participate for a good cause determination, sanction implementation or conciliation plans.

7.7 Employ or subcontract with staff as described in Subparagraph 14.2.1 of this Exhibit A that speak the CLIENTs' native languages and are culturally responsive to the populations served.

7.8 Encourage all CLIENTs, who meet the qualifications, to apply for CONTRACTOR staff positions to assist in reaching the goal of self-sufficiency.

7.9 Participate in Fair Hearings as necessary. Fair Hearings is a process available to CLIENTs if they disagree with an action taken by COUNTY.

7.10 Ensure CLIENT's Personally Personal Identifiable Information (PII) is kept confidential and secure in accordance with the County of Orange Social Services Agency (SSA) Administrative Policies and Procedures Manual policies Number I6, Information Technology Security and Usage and Number I7, Loss of Personally Identifiable Information, incorporated herein by reference as Attachments 1 and 2 respectively. CONTRACTOR acknowledges receipt of a copy of said policies.

7.11 CONTRACTOR shall comply with confidentiality requirements as stated in Paragraph 30 of this Agreement when accessing COUNTY Data System.

Further, CONTRACTOR shall provide training to staff that uses COUNTY Data System related to the sensitivity of Participant personal information.

8. REPORTING REQUIREMENTS

8.1 Reports

8.1.1 CONTRACTOR shall be responsible for submission of various reports, including but not limited to, financial reports, monthly progress reports, and a year-end final report. The year-end report will summarize the results of efforts made to achieve performance objectives, outcome measures and will reflect successes and barriers experienced in the provision of services.

8.1.2 CONTRACTOR shall:

8.1.2.1 Complete reports as required by ADMINISTRATOR, including Quarterly Performance, Quarterly Progress, and Semi-Annual Progress reports.

8.1.2.2 Comply with data gathering methodology as prescribed by ADMINISTRATOR.

8.1.2.3 Maintain and submit Employment Services and demographic statistics on CLIENTs served and services provided as required by ADMINISTRATOR

8.1.2.4 Maintain records, collect data, and provide reports as required by ADMINISTRATOR in order to track progress, and monitor outcome objectives identified in Subparagraph 5 of this Exhibit A. Data elements shall include, but are not limited to, the following:

8.1.2.5 Number of CLIENTs and breakdown of number of CLIENTs by age group, type of service and time elapsed from date of entry in the US;

8.1.2.6 Number of unduplicated CLIENTs placed into Employment Services as described in Subparagraph 6.1;

8.1.2.7 Number of unduplicated CLIENTs placed into Support Services as described in Subparagraph 6.1.7;

8.1.2.8 Number of unduplicated CLIENTs placed into Mentoring Services as described in Subparagraph 6.4;

8.1.2.9 Number of unduplicated CLIENTs placed into Citizenship and Naturalization Services as described in Subparagraph 6.5.1;

8.1.2.10 Percentage of unduplicated CLIENTs placed in either full or Part-Time employment;

8.1.2.11 Percentage of Job Placement with an average starting wage of at least eighteen percent (18%) above the prevailing California minimum wage;

8.1.2.12 Percentage of CLIENTs who retain employment for at least ninety (90) days;

8.1.2.13 Referrals made and referral outcomes: including subsidized child care and other supportive services;

8.1.2.14 Length of time placed in Employment Services;

8.1.2.15 Pay rate and length of time of employment retention;

8.1.2.16 Statistics regarding characteristics of identified segments of the refugee population;

8.1.2.17 Summary of complaints received;

8.1.2.18 Program Narrative: Will include activities undertaken to accomplish the annual outcome goals, as well as interim goals achieved within the reporting period, including new program initiative undertaken, plans developed and/or implemented for program improvement and service enhancement;

8.1.2.19 Outcomes of supervisory case reviews; and

8.1.2.20 Training activities and attendees.

8.2 Communication

8.2.1 Both parties agree that communication is essential to a CLIENT's success in achieving and maintaining economic self-sufficiency. CONTRACTOR shall communicate with ADMINISTRATOR and service providers as needed. Frequency of communication shall depend on the individual CLIENT/Family and specific service issue(s). After initial referral to a service provider, follow up communication shall be made with the CLIENT within seven (7) to ten (10) working days to ensure that link to the referred service was successful. All such communication shall be documented per Subparagraph 8.4.

8.2.2 Written communication shall be used to share case information or changes in a timely manner.

8.2.3 CONTRACTOR is required to maintain weekly contact with all CLIENTs in the caseload to better serve them as they move toward self-sufficiency. Ongoing contact with the CLIENT can serve to help the CONTRACTOR obtain necessary information, documentation, and to assess the CLIENT's needs. Types of expected contacts include, but are not limited to, face-to-face at the CONTRACTOR's office location, home visits, site visits with CLIENTs, letter/correspondence, and telephone contact.

8.2.4 All contacts should motivate and counsel CLIENTs in the benefits of economic self-sufficiency. Contacts should include, but are not limited to, gathering information needed to update the case, inquiring as to needs, and/or addressing and resolving identified CLIENT issues.

8.3 Forms

ADMINISTRATOR will provide a copy of all mandatory State and COUNTY forms. CONTRACTOR shall be responsible for duplication and distribution of the forms to its staff and any subcontractors. CONTRACTOR may develop their own internal forms that are not mandated by COUNTY, or by

program requirements. However, internal forms shall be reviewed and approved by ADMINISTRATOR prior to implementation.

8.4 Case Narratives

Narration is a vital part of the case record, and as such CONTRACTOR shall accurately maintain and update the case narrative. Case narratives shall be completed any time there is significant action taken by any staff person associated with the file. All entries by CONTRACTOR are to be signed, dated, legible, and in a format approved by ADMINISTRATOR. Case narratives shall include, but are not limited to, the following items:

8.4.1 Date case/referral is received;

8.4.2 Current status of the case, including assessment of service needs, actions taken, and status of referrals;

8.4.3 Scheduled date and reason for all contacts;

8.4.4 Overall plan of CLIENT contact, outcomes, and follow-up dates arranged during contact;

8.4.5 Participation hours;

8.4.6 Complete and accurate description of the case activity;

8.4.7 Issues related to the CLIENT's progress toward the goals established in the FSSP;

8.4.8 Identification of any missing information;

8.4.9 The closing narrative shall include date and reason for the case being closed and incomplete actions and reasons; and

8.4.10 Written or verbal communication with CLIENT.

9. PERFORMANCE MONITORING

9.1 Quality Control

CONTRACTOR shall establish and utilize a comprehensive Quality Control Plan, in a format approved by ADMINISTRATOR, to monitor the level of program services and quality. The Quality Control plan shall be submitted to

ADMINISTRATOR by November 1, 2017. The Quality Control Plan shall be in effect throughout the term of this Agreement and shall be updated as needed and submitted to ADMINISTRATOR for approval before changes are implemented.

9.1.1 The Quality Control Plan shall include, but not be limited to, the following:

9.1.1.1 The method for ensuring the services, deliverables, and requirements are being provided as defined in this Agreement;

9.1.1.2 The method for assuring that the professional staff rendering services under this Agreement have the necessary qualifications;

9.1.1.3 The method for assuring all staff receives initial and ongoing training for implementation of Paragraph 6 of this Exhibit A;

9.1.1.4 The method for identifying and preventing deficiencies in the quality of service;

9.1.1.5 The method for providing ADMINISTRATOR with a copy of CONTRACTOR case reviews, and a clear description of any corrective action taken to resolve identified problems;

9.1.1.6 Items/areas to be inspected on either a scheduled or unscheduled basis, how often inspections will be accomplished, and the title of the individual(s) who will perform the inspections;

9.1.1.7 Specific methods for identifying and preventing deficiencies in the quality of service performed, before the level of performance becomes unacceptable;

9.1.1.8 Maintenance of a file of all inspections conducted by CONTRACTOR and, if necessary, the corrective action taken; and

9.1.1.9 Method for continuing services in the event

of an emergency, such as a strike by CONTRACTOR's employees or a natural disaster.

9.2 Case Reviews and Audits

Case reviews and other inspection methods will be completed for compliance with COUNTY, State, or Federal requirements. Case reviews, data inspection, and audits may be completed by COUNTY, State, or Federal representatives. Cases that contain discrepancies or fail to meet RSS requirements may be referred back to CONTRACTOR for appropriate corrective action. CONTRACTOR shall be required to report proof of corrective action on all case errors and discrepancies. CONTRACTOR shall discuss the review with appropriate staff, control for corrective action, and address training issues. Case reviews include, but are not limited to:

9.2.1 Mandated reviews to meet State reporting requirements for RSS;

9.2.2 Reviews to meet Refugee Program Bureau requirements for RSS; and

9.2.3 COUNTY, State, and Federal audits.

9.3 Supervisor Reviews

CONTRACTOR's supervisors shall review a minimum of two (2) active cases per case carrying staff each month in a format approved by ADMINISTRATOR. Cases shall be randomly selected per a method determined by ADMINISTRATOR. Supervisor reviews shall include, but not be limited to:

9.3.1 Overall case management and application of RSS rules and regulations.

9.3.2 CLIENT's participation hours, case discrepancies, and any other identified corrective actions required.

9.3.3 Narration (s) in the case record, including, but not limited to:

9.3.3.1 Summary of the case review findings, and

9.3.3.2 Strategy recommendations to assist the CLIENT in achieving FSSP positive outcomes.

9.4 Contractor Performance Monitoring

CONTRACTOR's performance shall be monitored and reviewed by ADMINISTRATOR who will conduct reviews as part of an on-going evaluation of CONTRACTOR's performance. CONTRACTOR shall cooperate with ADMINISTRATOR in providing the information necessary for monitoring CONTRACTOR's performance under this Agreement. ADMINISTRATOR may use a variety of inspection methods to evaluate CONTRACTOR's performance, including, but not be limited to, the following:

9.4.1 Monthly reviews of CONTRACTOR's case management performance and implementation of best practices to achieve outcomes. ADMINISTRATOR will review CONTRACTOR cases and applicable data reports to ensure compliance with the RSS requirements:

9.4.2 Periodic site visits;

9.4.3 Random sampling of program activities including a review of case files each month;

9.4.4 Activity checklists and random observations;

9.4.5 Inspection of output items on a periodic basis as deemed necessary;

9.4.6 Review of CONTRACTOR's statistical reports;

9.4.7 RSS participant complaints; and

9.4.8 Service provider complaints or reports.

9.4.9 When it is determined that services were not performed in accordance with the requirements of this Agreement during the review period, ADMINISTRATOR may require corrective action plans. CONTRACTOR shall, within the time period specified in any such corrective action plan, remedy the

performance defects. Performance evaluation meetings will be conducted as deemed necessary by ADMINISTRATOR. Nothing in this section shall limit the COUNTY's ability to terminate this agreement pursuant to Paragraph 42.

9.5 Handling Complaints

CONTRACTOR shall:

9.5.1 Develop, operate and maintain procedures for receiving, investigating and responding to provider and CLIENT complaints, including Civil Rights complaints, requests for reviews by ADMINISTRATOR, negative comments and other complaints relating to services provided under this Agreement.

9.5.2 Maintain a log for identification and response to CLIENTs' complaints. When complaints cannot be resolved informally, a system of follow-through shall be instituted which adheres to formal plans for specific actions. Responses to complaints should occur within two (2) business days, unless otherwise authorized by ADMINISTRATOR.

9.5.3 For Civil Rights complaints, refer to Subparagraph 8.6.2 of this Agreement.

9.5.4 When CONTRACTOR believes any complaint may have legal implications for CONTRACTOR or COUNTY, CONTRACTOR shall forward such complaint immediately to ADMINISTRATOR prior to responding to the complaint. In the event any such complaint pertains to an injury or property damage, CONTRACTOR shall follow the provisions as set forth in Subparagraph 13.1 of this Agreement.

9.5.5 CONTRACTOR shall provide to ADMINISTRATOR, in a form approved by ADMINISTRATOR, information pertaining to complaints, as well as CONTRACTOR's response to any complaints as described above within ten (10) business days of the complaint, except as provided in Subparagraph 9.5.4. CONTRACTOR shall provide a summary of all complaints and/or negative comments

as prescribed and on a format approved by ADMINISTRATOR. Complaints include, but are not limited to, complaints from CLIENTs, other COUNTY contracted service providers, community organizations, and the public.

9.6 Fraud Investigation Referrals

If RCA eligibility fraud is suspected, CONTRACTOR staff shall inform ADMINISTRATOR within 48 hours of awareness of any suspected fraud.

9.7 Formal Grievance Process and State Hearing

9.7.1 CONTRACTOR shall inform each CLIENT of his or her grievance, State Hearing and Civil Rights, and of his or her right to request a review by a COUNTY worker of a grievance should the CLIENT disagree with an action made by the CONTRACTOR.

9.7.2 Grievance Rights and Civil Rights notices, in multiple languages, shall be posted in RSS office(s) where all CLIENTs can easily see them, in accordance with Subparagraph 8.6 of this Agreement.

9.7.3 CONTRACTOR shall attend COUNTY Formal Grievance Hearings and State Hearings when requested, and comply with the decisions of the Hearing Officers. All actions involving the Formal Grievance Process and State Hearings shall be properly documented by CONTRACTOR.

10. OUTSIDE CONTACTS

CONTRACTOR shall:

10.1 Immediately inform ADMINISTRATOR of any inquiry from an elected official, their representative, participant representative, or the press, and immediately provide information in order for ADMINISTRATOR to respond.

10.2 Consult with ADMINISTRATOR prior to initiating contact with a participant representative or the press.

10.3 Inform ADMINISTRATOR prior to initiating contact with an elected official or their representative.

///

11. COORDINATION

11.1 CONTRACTOR must jointly host regular coordination meetings with ADMINISTRATOR and CONTRACTOR's staff to coordinate procedures, review program operations, and solve problems.

12. FACILITY

CONTRACTOR shall:

12.1 Provide its own facility for CONTRACTOR's administrative functions and programmatic functions of administering services pursuant to this Agreement. COUNTY has the right to approve or disapprove of CONTRACTOR's facility and location;

12.2 Ensure that proposed facility location(s) are accessible to public transportation for CLIENTs from throughout Orange County;

12.3 Not require participants to travel more than two (2) hours round trip to obtain services;

12.4 Maintain an Accessibility Plan that describes how participants located throughout Orange County can easily get to the sites;

12.5 Provide parking spaces for participants' free and exclusive use;

12.6 Provide parking for disabled persons in accordance with the Americans with Disabilities Act, and any other rules or statutes relating to parking for disabled persons;

12.7 CONTRACTOR shall provide space for the provision of services under this Agreement at the minimum at the following site:

631 S. Brookhurst Street Suite 107, Anaheim CA 92804

12.8 CONTRACTOR's facilities shall be safe, clean structures and maintained in compliance with all applicable laws, rules, regulations, building codes, statutes, and orders, as they now exist or may be subsequently amended. CONTRACTOR shall provide all repair, maintenance, and janitorial services to all premises on a five-day-per-week basis, subject to the

satisfaction of COUNTY. If CONTRACTOR fails to provide satisfactory repair, maintenance, and janitorial services to the premises, ADMINISTRATOR may notify CONTRACTOR in writing. Failure to comply shall result in termination of this Agreement;

12.9 CONTRACTOR and ADMINISTRATOR may mutually agree in writing as to the facility (ies) and location(s) where services shall be provided without changing COUNTY's maximum obligation.

13. BUDGET

The budget for services provided pursuant to Exhibit A of this Agreement shall span thirty-six (36) months and is set forth as follows:

Budget for Period of October 1, 2017 through September 30, 2018:

SALARIES AND EMPLOYEE BENEFITS	
Direct Service Positions [3]	
Subtotal Direct Service Positions	366,402
Benefits [1]	58,624
Subtotal Direct Service Positions and Benefits	$425,026
Administrative Positions[2]	
Subtotal Administrative Salaries	13,906
Benefits [1]	2,225
Subtotal Administrative Salaries and Benefits	$16,131
TOTAL SALARIES & EMPLOYEE BENEFITS	$441,157
Services and Supplies	
Services	$3,000
Supplies	$6,533
TOTAL SERVICES and SUPPLIES	$9,533
Operating Expenses	
Operating Expenses	$49,310
TOTAL SERVICES AND SUPPLIES AND OPERATING EXPENSES	$58,843

TOTAL ALLOWABLE COSTS October 1, 2017 through September 30, 2018	$500,000
Budget for Period of October 1, 2018 through September 30, 2019:	
SALARIES AND EMPLOYEE BENEFITS	
Direct Service Positions [3]	
Subtotal Direct Service Positions	366,402
Benefits [1]	58,624
Subtotal Direct Service Positions and Benefits	$425,026
Administrative Positions[2]	
Subtotal Administrative Salaries	13,906
Benefits [1]	2,225
Subtotal Administrative Salaries and Benefits	$16,131
TOTAL SALARIES & EMPLOYEE BENEFITS	$441,157
Services and Supplies	
Services	$3,000
Supplies	$6,533
TOTAL SERVICES and SUPPLIES	$9,533
Operating Expenses	
Operating Expenses	$49,310
TOTAL SERVICES AND SUPPLIES AND OPERATING EXPENSES	$58,843
TOTAL ALLOWABLE COSTS October 1, 2018 through September 30, 2019	$500,000
Budget for Period of October 1, 2019 through September 30, 2020:	
SALARIES AND EMPLOYEE BENEFITS	
Direct Service Positions [3]	
Subtotal Direct Service Positions	366,402
Benefits [1]	58,624
Subtotal Direct Service Positions and Benefits	$425,026
Administrative Positions[2]	
Subtotal Administrative Salaries	13,906

Benefits [1]	2,225
Subtotal Administrative Salaries and Benefits	$16,131
TOTAL SALARIES & EMPLOYEE BENEFITS	$441,157
Services and Supplies	
Services	$3,000
Supplies	$6,533
TOTAL SERVICES and SUPPLIES	$9,533
Operating Expenses	$49,310
TOTAL SERVICES AND SUPPLIES AND OPERATING EXPENSES	$58,843
TOTAL ALLOWABLE COSTS October 1, 2019 through September 30, 2020	$500,000
TOTAL MAXIMUM OBLIGATION for the period of October 1, 2017 through September 30, 2020	$1,500,000

[1] Employee Benefits include health, dental, life and disability insurance. Also included are payroll taxes such as FICA, Federal Unemployment Tax, State Unemployment Tax, and Worker's Compensation Tax, based on the currently prevailing rates, not to exceed sixteen percent (16%) of actual allowable costs of direct service salaries and sixteen percent (16%) of actual allowable costs of administrative salaries.

[2] Administrative positions are defined as all other classifications either higher than first line supervisors or positions not providing services to CLIENTs. Administrative positions higher than first line supervisors must be specified as either salaried or hourly positions.

[3] Direct Service positions are defined as those staff that provides face to face contact with clients. First line supervisors can be included as direct service staff. All direct staff positions are to be compensated hourly.

13.1 Administrative costs are defined as those costs not solely related to direct services to CLIENTs, supervision and program costs (e.g., executive director oversight, technology services, accounting, payroll, etc.) shall be held to no more than fifteen (15%) percent of total gross program costs.

13.2 CONTRACTOR and ADMINISTRATOR may agree, subject to advance written notice, to add, delete or modify line items without changing COUNTY's maximum obligation as stated in Subparagraph 19.1 of this Agreement or reducing the

level of service to be provided by CONTRACTOR. Further, in accordance with Subparagraph 42 of this Agreement, in the event ADMINISTRATOR reduces the maximum obligation as stated in Subparagraph 19.1 , CONTRACTOR and ADMINISTRATOR may mutually agree in writing to proportionately reduce the service goals as set forth in this Exhibit.

14. CONTRACTOR STAFF

14.1 Recruitment and Hiring Practices

14.1.1 CONTRACTOR shall use a formal recruitment plan, which complies with Federal and State employment and labor regulations. CONTRACTOR shall hire staff with the education and experience necessary to appropriately perform all functions.

14.1.2 CONTRACTOR shall give priority consideration to qualified job-ready RSS CLIENTs when filling vacant positions funded by this Agreement.

14.2 Language Diversity

14.2.1 CONTRACTOR shall employ or subcontract staff with experience in placing CLIENTs with a limited English vocabulary in an environment that facilitates the development of the English language. CONTRACTOR's staff shall be able to read, write, speak, and understand English. CONTRACTOR shall provide bilingual staff to serve CLIENTs in the language they speak. The ratio of bilingual staff shall be consistent with and proportional to the target population, as determined by ADMINISTRATOR. In addition, CONTRACTOR shall be required to provide translation services for all other languages as needed to ensure all participants are provided services in the language they speak.

14.2.2 CONTRACTOR shall comply with all COUNTY, State, and Federal regulations regarding Limited English Proficiency (LEP). LEP regulations affect anyone who participates in a Federally funded program, and who has English as his or her second language and is limited in his or her

English language proficiency.

14.3 Staff Training

14.3.1 CONTRACTOR's staff directly serving CLIENTs/Families, or supervising those who do, shall be thoroughly familiar with RSS rules and regulations contained in the current Orange County Refugee Services Plan, SSA policies and related instructions, welfare fraud and child abuse/elder abuse reporting requirements, the State Hearing process, and Civil Rights compliance requirements.

14.3.2 ADMINISTRATOR will provide instructions, guidelines, and RSS rules and regulations to CONTRACTOR during start-up, and subsequently as these materials are revised or new policies are developed.

14.3.3 ADMINISTRATOR will provide initial training to a limited number of select CONTRACTOR staff with respect to ADMINISTRATOR's instructions, guidelines, and RSS rules and regulations; CONTRACTOR shall conduct subsequent training(s).

14.3.4 CONTRACTOR shall be required to attend training(s) and/or meetings that ADMINISTRATOR determines to be mandatory, and provide CONTRACTOR staff with ongoing training and assistance to ensure that requirements of this Agreement are met. All training materials developed by CONTRACTOR shall be approved by ADMINISTRATOR in advance of training.

14.3.5 CONTRACTOR shall ensure that CONTRACTOR staff, as described above, receives training in understanding the cultural differences among groups of CLIENTs, and recognizes and effectively intervenes to overcome any language and/or cultural barriers to employment.

14.3.6 CONTRACTOR shall maintain a log of in-house training activities and the staff that attended. This log shall be made available to ADMINISTRATOR upon request.

///

15. STAFF POSITIONS

CONTRACTOR shall provide the following staff positions. Any employment experience allowed as a substitute for education requirements in accordance with the minimum qualifications as stated for each staff position below, shall be in addition to the minimum experience required as stated for the staff position.

15.1 Program Director

15.1.1 Duties

15.1.1.1 Oversee all segments of the RSS program;

15.1.1.2 Supervise Program Manager and provide necessary coverage in his/her absence;

15.1.1.3 Attend all County meetings and trainings;

15.1.1.4 Validate monthly and annual statistical data and reports; complete RS-50 monthly and quarterly reports and deliver to ADMINISTRATOR;

15.1.1.5 Ensure RSS program is implemented according to contract;

15.1.1.6 Complete internal evaluations to constantly enhance program deliverables;

15.1.1.7 Present EPW as required;

15.1.1.8 Collaborate with Executive Director to hire RSS staff; and

15.1.1.9 Collaborate with other service providers to strengthen and expand the RSS program.

15.1.2 Qualifications

15.1.2.1 A minimum of two (2) years of experience in a human services related field. Experience working with the refugee community is preferred.

15.1.2.2 Bachelor's degree from an accredited college or university, preferably in a human services field. Two (2) years of course work in an accredited college or university plus two (2) years of employment experience, preferably in a human services field, may substitute for the Bachelor's degree.

15.2 Program Manager

15.2.1 Duties

15.2.1.1 Supervise Supervisor I/II and provide necessary coverage in their absence;

15.2.1.2 Complete monthly statistical data and reports, regularly review CLIENT files

15.2.1.3 Attend all County meetings and trainings; regularly meet with AGENCY staff to relay new regulations, data collection changes and/or new reporting procedures;

15.2.1.4 Ensure the Quality Control Plan is implemented;

15.2.1.5 Frequently present EPW;

15.2.1.6 Interact with CLIENTs in Client Complaint/Grievance Process Level III to mitigate CLIENT complaints if needed;

15.2.1.7 Report to Program Director.

15.2.2 Qualifications

15.2.2.1 A minimum of one (1) year of experience in a human services related field. Experience working with the refugee community is preferred.

15.2.2.2 Bachelor's degree from an accredited college or university preferably in a human services related field. Two (2) years of course work in an accredited college or university plus two (2) years of employment experience, preferably in a human services field, may substitute

for the Bachelor's degree.

15.2.2.3 Competent in using personal computers and Microsoft Office.

15.2.2.4 Bilingual capabilities in one or more of the languages spoken by CLIENTS served pursuant to this Agreement.

15.2.2.5 Possess excellent organizational, interpersonal, written, and verbal communication skills; ability to perform comfortably in a fast-paced, deadline oriented work environment; ability to successfully execute many complex tasks simultaneously; and ability to work as a team member, as well as independently.

15.3 Supervisor I/II

15.3.1 Duties

15.3.1.1 Supervise Intake Clerks, Case Managers and Job Developer I/II and provide necessary coverage in their absence.

15.3.1.2 Complete CLIENT Home Visits upon acceptance, identify and attempt to mitigate household barriers, address CLIENT's needs to improve his or her quality of life.

15.3.1.3 Attend trainings pertaining to RSS Program and the refugee community.

15.3.1.4 Provide training for Case Managers on new skills learned from trainings attended.

15.3.1.5 Review case records and FSSP for completeness, accuracy, consistency, and conformity with RSS requirements, regulations, and policies and proper case management practices; and discuss cases with the Case Managers to suggest and recommend methods of resolving issues.

15.3.1.6 Frequently present EPW.

15.3.1.7 Interact with CLIENTs in Client

Complaint/Grievance Process Level II to mitigate CLIENT complaints if needed.

15.3.1.8 Report to Program Manager.

15.3.2 Qualifications

15.3.2.1 A minimum of one (1) year of experience working with the refugee community.

15.3.2.2 Bachelor's degree from an accredited college or university, preferably in a human services related field. Four (4) years of experience in employment services or human services may substitute for the Bachelor's degree.

15.3.2.3 Competent in the use of personal computers and knowledgeable in the use of word processing and spreadsheet programs such as Microsoft Word and Excel.

15.3.2.4 Bilingual capabilities in one or more of the refugee languages spoken by CLIENTs served pursuant to this Agreement.

15.3.2.5 Possess organizational, interpersonal, written, and verbal communication skills; ability to perform comfortably in a fast-paced, deadline oriented work environment; ability to successfully execute many complex tasks simultaneously; and ability to work as a team member, as well as independently.

15.4 Job Developer I/II

15.4.1 Duties

15.4.1.1 Work closely with Case Manager and CLIENT to formalize a customized job readiness plan;

15.4.1.2 Complete regular individualized sessions to refine CLIENT resumes, enhance interviewing skills and eventually linking CLIENT to suitable employers; and

15.4.1.3 Prepare and present EPW, maintains workshop topic database, coordinate and invite guest speakers to improve upon and

engage audiences.

15.4.1.4 Report to Supervisor I/II

15.4.2 Qualifications

15.4.2.1 A minimum of one (1) year of work experience in a human services related field and a minimum of one year of work experience in program evaluation. The minimum work experience may be concurrent with one position. Experience working with the refugee community is preferred.

15.4.2.2 Bilingual capabilities in one or more of the languages spoken by the refugee CLIENTs served pursuant to this Agreement.

15.5 Case Manager

15.5.1 Duties

15.5.1.1 Conduct Intake and Assessment Interviews with CLIENTs; work directly with CLIENTs to develop and implement FSSP; conduct home visits to assess Families and monitor progress; and follow-up to ensure services are received and goals are achieved.

15.5.1.2 Document all actions taken in case file.

15.5.1.3 Complete CLIENT orientation, identifies employment barriers, administer Pre and Post BEST Tests to determine CLIENT SPL scores and qualify them into either VESL or EPW track.

15.5.1.4 Coordinate delivery of VESL and citizenship instruction classes; present EPW.

15.5.1.5 Provide post-employment follow ups to monitor job adjustments and satisfaction.

15.5.1.6 Report to Supervisor I/II

15.5.2 Qualifications

15.5.2.1 Bachelor's degree from an accredited college or university, preferably in a human services related field. Four (4) years of experience in employment services or human services may substitute for the

Bachelor's degree.

15.5.2.2 Competent in the use of personal computers and knowledgeable in the use of word processing and spreadsheet programs such as Microsoft Word and Excel.

15.5.2.3 Bilingual capabilities in one or more of the refugee languages spoken by CLIENTs served pursuant to this Agreement.

15.5.2.4 Possess organizational, interpersonal, written, and verbal communication skills; ability to perform comfortably in a fast-paced, deadline oriented work environment; ability to successfully execute many complex tasks simultaneously; and ability to work as a team member, as well as independently.

15.6 Intake Clerk

15.6.1 Duties

15.6.1.1 Accept all referrals from SSA, public or private agencies and self-referred aided or non-aided CLIENT.

15.6.1.2 Verify initial eligibility

15.6.1.3 Assign Case Manager to each CLIENT

15.6.1.4 Report to Supervisor I/II

15.6.2 Qualifications

15.6.2.1 High School diploma and/or General Education Diploma (GED) or a minimum of three (3) months of related experience preferably in a human services field and /or training in an office setting.

15.6.2.2 Excellent written and oral skills. Knowledge of Microsoft Office suite tools, emails and operating copy machines and fax.

15.7 Van Driver

15.7.1 Duties

15.7.1.1 Provide transportation to CLIENTs, utilizing CONTRACTOR's vehicle, for ES, including but not limited to the following:

classes, interviews, job fairs, and all related activities pertaining to ES.

15.7.1.2 Perform preventive and regular maintenance on vehicle.

15.7.2 Qualifications

15.7.2.1 Must be at least twenty-one (21) years old with a valid Class C California license.

15.7.2.2 Meet all Department of Transportation requirements and physical demands on the job description.

15.7.2.3 Have a verifiable and stable work history and references; no major preventable accident within the past three (3) years; no felony convictions; no more than three (3) moving violations in the past three (3) years; no serious violation in the past twelve (12) months; no more than six (6) moving violations in a lifetime.

15.7.2.4 No DUI or DWI convictions.

15.8 Executive Director

15.8.1 Duties

15.8.1.1 Provide overall leadership and administrative support for agency, including program oversight, financial management, and community relations and networking.

15.8.1.2 Supervise and oversee all reporting requirements completed by Program Director; provide necessary coverage in his/her absence.

15.8.1.3 Reports all RSS Program information to the Board of Directors.

15.8.2 Qualifications

15.8.2.1 A minimum of two (2) years of experience in a human services related field. Experience working with the refugee community is preferred.

EXHIBIT B

TO

AGREEMENT

BETWEEN

COUNTY OF ORANGE

AND

ACCESS CALIFORNIA SERVICES

FOR THE PROVISION OF REFUGEE SOCIAL SERVICES

AND

REFUGEE HEALTH SERVICES

1. DEFINITIONS

1.1 EDN - The Electronic Disease Notification System is the Centers for Disease Control and Prevention's (CDC) web-based system that automates the process that notifies state or local health officials of the arrival of refugees and immigrants with notifiable conditions to their jurisdictions. EDN provides relevant overseas medical screening and treatment information for stateside follow-up.

1.2 Health Assessment - Completion of a RHAP health assessment is defined as having laboratory testing completed, a physical examination, and having results provided to the individual and appropriate referrals completed.

1.3 ORR - The federal Office of Refugee Resettlement (ORR) funds designated resettlement agencies, which help refugees become self-sufficient as quickly as possible after their arrival in the United States. ORR also provides funds through the California Department of Public Health (CDPH) Refugee Health Assessment Program (RHAP), for the County to provide comprehensive health assessments to incoming refugees and other eligible individuals.

1.4 RAs -Resettlement Agencies are non-profit organizations that provide sponsorship and initial resettlement services for refugees entering the United States (US).

1.5 RHAP - Refugee Health Assessment Program services are determined by ORR and CDPH Office of Refugee Health. Eligibility may vary over time, but the majority of eligible clients will be newly entering refugees, secondary migrants who have entered as refugees in another US state or County but did not have an entry examination, granted asylees, Cuban and Haitian entrants, Cuban medical professionals and their spouses and children, certain Amerasians from Vietnam, victims of severe forms of trafficking who receive certification or an eligibility letter from the ORR and certain other specified family members of trafficking victims, and Iraqi and Afghan citizens with Special Immigrant Visa (SIV) status.

1.6 RHEIS - Refugee Health Electronic Information System is the State database used to collect key elements of the RHAP assessment.

1.7 TB Classification - for RHEIS, Tuberculosis (TB) classification refers to categories defined by the American Thoracic Society to characterize tuberculosis status. Class 0 = No exposure, no infection; Class 1 = Exposure, no infection; Class 2 = Latent TB infection; Class 3 = TB disease, Class 4 = Inactive TB; Class 5 = TB disease suspected.

1.8 TB Classification, oversees - On overseas examinations, refers to categories defined by the CDC to characterize specific TB status. Class B1 = possible active TB; B2 LTBI = latent TB infection; B3 = contact to an active TB case while overseas.

2. CATALOG OF FEDERAL DOMESTIC ASSISTANCE (CFDA) INFORMATION

2.1 This Agreement includes federal funds paid to CONTRACTOR. The CFDA number(s) and associated information for federal funds paid through this Agreement are specified below:

CFDA Year: 2017

CFDA No.: 93.566

Program Title: Refugee and Entrant Assistance - State Administered Programs

Federal Agency: Department of Health and Human Services Administration for Children and Families

Award Name: Refugee Cash and Medical Assistance Program and Refugee Social Services Program

Amount: $214,300 (estimated per year)

2.2 HCA may revise the CFDA information listed above, and shall notify CONTRACTOR in writing of said revisions.

3. FACILITY

3.1 CONTRACTOR shall maintain a service site, preferably multiple sites, within walking distance to public transportation, located in Orange County that meets the following minimum requirements:

3.1.1 A waiting room;

3.1.2 Minimum of one (1) patient examination room for performance of health assessments; and

3.1.3 Capable of handling family units who present for service at the same time.

3.2 CONTRACTOR shall:

3.2.1 Provide its own facility for CONTRACTOR's administrative functions and programmatic functions of administering services pursuant to this Agreement. COUNTY has the right to approve or disapprove of CONTRACTOR's facility and location;

3.2.2 Ensure that proposed facility location(s) are accessible to public transportation for clients from throughout Orange County;

3.2.3 Not require participants to travel more than two

(2) hours round trip to obtain services;

3.2.4 Maintain an Accessibility Plan that describes how participants located throughout Orange County can easily get to the sites;

3.2.5 Provide parking spaces for participants' free and exclusive use;

3.2.6 Provide parking for disabled persons in accordance with the Americans with Disabilities Act, and any other rules or statutes relating to parking for disabled persons;

3.2.7 CONTRACTOR shall provide space for the provision of services under this Agreement at the minimum at the following site:

631 S. Brookhurst Street Suite 107, Anaheim CA 92804

3.2.8 CONTRACTOR's facilities shall be safe, clean structures and maintained in compliance with all applicable laws, rules, regulations, building codes, statutes, and orders, as they now exist or may be subsequently amended. CONTRACTOR shall provide all repair, maintenance, and janitorial services to all premises on a five-day-per-week basis, subject to the satisfaction of COUNTY. If CONTRACTOR fails to provide satisfactory repair, maintenance, and janitorial services to the premises, HCA may notify CONTRACTOR in writing. Failure to comply shall result in termination of this Agreement;

3.2.9 CONTRACTOR and HCA may mutually agree in writing as to the facility (ies) and location(s) where services shall be provided without changing COUNTY's maximum obligation.

3.3 CONTRACTOR and HCA may mutually agree to modify the FACILITY section of this Exhibit B to the Agreement. Any modification must be in writing.

4. HOURS OF OPERATION

4.1 CONTRACTOR shall provide service hours that are responsive to the

needs of the target population(s) as determined by HCA. At a minimum, CONTRACTOR must provide services Monday through Friday, from 8:00 a.m. to 5:00 p.m., except COUNTY holidays as established by the Orange County Board of Supervisors. However, CONTRACTOR is encouraged to provide the contracted services on holidays, whenever possible.

4.2 CONTRACTOR's holiday schedule shall not exceed COUNTY's holiday schedule which is as follows: New Year's Day, Martin Luther King Day, President Lincoln's Birthday, Presidents' Day, Memorial Day, Independence Day, Labor Day, Columbus Day, Veterans Day, Thanksgiving Day, Friday after Thanksgiving, and Christmas Day. CONTRACTOR shall obtain prior written approval from HCA for any closure outside of COUNTY's holiday schedule or the hours in Paragraph 4.1. Any unauthorized closure shall be deemed a material breach of this Agreement, pursuant to Paragraph 18, and shall not be reimbursed.

5. PAYMENTS

5.1 COUNTY shall pay CONTRACTOR quarterly, in arrears, in the amount of $53,575 throughout the term of the Agreement. Upon receipt of an invoice in a form acceptable to COUNTY, provided the total of such payments shall not exceed COUNTY's Maximum Obligation as specified in the Contract Provisions of the Agreement.

5.2 CONTRACTOR's billings shall be on a form approved or provided by SSA and provide such information as is required by SSA. Billings are due by the twentieth (20th) calendar day of each quarter following the month in which services were performed under the Agreement. Invoices received after the due date may not be paid within the same month. COUNTY should release payments to CONTRACTOR no later than twenty-one (21) business days after receipt of the correctly completed billing form.

5.3 All billings to COUNTY shall be supported, at CONTRACTOR's

facility, by source documentation including, but not limited to, ledgers, journals, time sheets, invoices, bank statements, canceled checks, receipts, receiving records and records of services provided.

5.4 At SSA's sole discretion, SSA may withhold or delay all or a part of any payment if CONTRACTOR fails to comply with any provision of the Agreement.

5.5 COUNTY shall not reimburse CONTRACTOR for services provided beyond the expiration and/or termination of the Agreement, except as may otherwise be provided under the Agreement, or specifically agreed upon in a subsequent Agreement.

5.6 CONTRACTOR and SSA may mutually agree to modify the Payments Paragraph of this Exhibit B to the Agreement. Any modification must be in writing.

6. EXPENDITURE REPORT

6.1 No later than sixty (60) calendar days following termination of each period or fiscal year of this Agreement, CONTRACTOR shall submit to SSA, for informational purposes only, an Expenditure Report for the preceding fiscal year, or portion thereof. Such report shall be prepared in accordance with the procedure that is provided by SSA and GAAP.

6.2 CONTRACTOR may be required to submit periodic Expenditure Reports throughout the term of this Agreement.

7. PERFORMANCE OBJECTIVES

7.1 CONTRACTOR shall meet the following performance objectives, which shall be calculated quarterly, for each term of the contract

7.1.1 Ensure that ninety percent (90%) of all arriving refugees and sixty percent (60%) of all arriving asylees, Cuban/Haitian entrants, federally-certified victims of human trafficking, and other eligible entrants start the health assessment process.

7.1.2 Ensure that ninety percent (90%) of individuals who start the health assessment process have a completed health assessment within ninety (90) days from date of US arrival, date parole status is granted, date asylum status is granted, or date of certification.

7.1.3 Assess immunization status of ninety-five percent (95%) of individuals who have started a health assessment, according to the most current Requirements for Routine Vaccination of Adjustment of Status Applicants.

7.1.4 Ensure that ninety-five percent (95%) of individuals identified as eligible to receive scheduled immunizations at the time of the health assessment are either immunized or referred to an appropriate provider.

7.1.5 Ensure that ninety-five (95%) of individuals identified with a health condition needing further medical evaluation are informed of their conditions at the time of physical examination and treated or referred to a health care provider for treatment.

7.1.6 Ensure that ninety-five (95%) of arrivals with a positive TB skin or blood test are evaluated for TB infection or disease and classified accordingly.

7.1.7 Ensure that eighty (80%) of individuals recommended to commence latent TB infection treatment are started on therapy, and that 70% of those commencing treatment complete therapy.

7.2 CONTRACTOR and HCA may mutually agree to modify the Performance Objectives Paragraph of this Exhibit B to the Agreement. Any modification must be in writing.

8. COMPLIANCE

8.1 HCA has established a Compliance Program for the purpose of ensuring adherence to all rules and regulations related to federal and state

health care programs.

8.1.1 HCA shall provide CONTRACTOR with a copy of the relevant HCA policies and procedures relating to HCA's Compliance Program, HCA's Code of Conduct and General Compliance Trainings.

8.1.2 CONTRACTOR has the option to adhere to HCA's Compliance Program and Code of Conduct or establish its own, provided CONTRACTOR's Compliance Program and Code of Conduct have been verified to include all required elements by HCA's Compliance Officer as described in subparagraphs below.

8.1.3 If CONTRACTOR elects to adhere to HCA's Compliance Program and Code of Conduct; the CONTRACTOR shall submit to the HCA within thirty (30) calendar days of award of this Agreement a signed acknowledgement that CONTRACTOR shall comply with HCA's Compliance Program and Code of Conduct.

8.1.4 If CONTRACTOR elects to have its own Compliance Program and Code of Conduct then it shall submit a copy of its Compliance Program, Code of Conduct and relevant policies and procedures to HCA within thirty (30) calendar days of award of this Agreement. HCA's Compliance Officer shall determine if CONTRACTOR Compliance Program and Code of Conduct contains all required elements. CONTRACTOR shall take necessary action to meet said standards or shall be asked to acknowledge and agree to the HCA's Compliance Program and Code of Conduct if the CONTRACTOR Compliance Program and Code of Conduct does not contain all required elements.

8.1.5 Upon written confirmation from HCA's Compliance Officer that the CONTRACTOR Compliance Program and Code of Conduct contains all required elements, CONTRACTOR shall ensure that all Covered Individuals relative to this Agreement are made aware of CONTRACTOR's Compliance Program, Code of Conduct and related policies and procedures.

8.1.6 Failure of CONTRACTOR to submit its Compliance Program, Code of Conduct and relevant policies and procedures shall constitute a material breach of this Agreement.

8.2 SANCTION SCREENING - CONTRACTOR shall adhere to all screening policies and procedures and screen all Covered Individuals employed or retained to provide services related to this Agreement to ensure that they are not designated as Ineligible Persons, as pursuant to this Agreement. Screening shall be conducted against the General Services Administration's Excluded Parties List System or System for Award Management, the Health and Human Services/Office of Inspector General List of Excluded Individuals/Entities, and the California Medi-Cal Suspended and Ineligible Provider List and/or any other as identified by the HCA.

8.2.1 Covered Individuals includes all contractors, subcontractors, agents, and other persons who provide health care items or services or who perform billing or coding functions on behalf of HCA. Notwithstanding the above, this term does not include part-time or per-diem employees, contractors, subcontractors, agents, and other persons who are not reasonably expected to work more than one hundred sixty (160) hours per year; except that any such individuals shall become Covered Individuals at the point when they work more than one hundred sixty (160) hours during the calendar year. CONTRACTOR shall ensure that all Covered Individuals relative to this Agreement are made aware of HCA's Compliance Program, Code of Conduct and related policies and procedures.

8.2.2 An Ineligible Person shall be any individual or entity who:

8.2.2.1 Is currently excluded, suspended, debarred or otherwise ineligible to participate in federal and state health care programs; or

8.2.2.2 Has been convicted of a criminal offense related to the provision of health care items or services and has not been reinstated in the federal and state health care programs after a period of exclusion, suspension, debarment, or ineligibility.

8.2.3 CONTRACTOR shall screen prospective Covered Individuals prior to hire or engagement. CONTRACTOR shall not hire or engage any Ineligible Person to provide services relative to this Agreement.

8.2.4 CONTRACTOR shall screen all current Covered Individuals and subcontractors semi-annually to ensure that they have not become Ineligible Persons. CONTRACTOR shall also request that its subcontractors use their best efforts to verify that they are eligible to participate in all federal and State of California health programs and have not been excluded or debarred from participation in any federal or state health care programs, and to further represent to CONTRACTOR that they do not have any Ineligible Person in their employ or under contract.

8.2.5 Covered Individuals shall be required to disclose to CONTRACTOR immediately any debarment, exclusion or other event that makes the Covered Individual an Ineligible Person. CONTRACTOR shall notify HCA immediately if a Covered Individual providing services directly relative to this Agreement becomes debarred, excluded or otherwise becomes an Ineligible Person.

8.2.6 CONTRACTOR acknowledges that Ineligible Persons are precluded from providing federal and state funded health care services by contract with COUNTY in the event that they are currently sanctioned or excluded by a federal or state law enforcement regulatory or licensing agency. If CONTRACTOR becomes aware that a Covered Individual has become an Ineligible Person, CONTRACTOR shall remove such individual from responsibility for, or involvement with, COUNTY business operations related to this Agreement.

8.2.7 CONTRACTOR shall notify HCA immediately if a Covered Individual or entity is currently excluded, suspended or debarred, or is identified as such after being sanction screened. Such individual or entity shall be immediately removed from participating in any activity associated with this Agreement. HCA will determine appropriate repayment from, or sanction(s) to CONTRACTOR for services provided by ineligible person or individual. CONTRACTOR shall promptly return any overpayments within forty-five (45) business days after the overpayment is verified by the HCA.

8.3 COMPLIANCE TRAINING - HCA shall make General Compliance Training and Provider Compliance Training, where appropriate, available to Covered Individuals.

8.3.1 CONTRACTOR shall use its best efforts to encourage completion by Covered Individuals; provided, however, that at a minimum CONTRACTOR shall assign at least one (1) designated representative to complete all Compliance Trainings when offered.

8.3.2 Such training will be made available to Covered Individuals within thirty (30) calendar days of employment or engagement.

8.3.3 Such training will be made available to each Covered Individual annually.

8.3.4 Each Covered Individual attending training shall certify, in writing, attendance at compliance training. CONTRACTOR shall retain the certifications. Upon written request by HCA, CONTRACTOR shall provide copies of the certifications.

8.4 MEDICAL BILLING, CODING, AND DOCUMENTATION COMPLIANCE STANDARDS

8.4.1 CONTRACTOR shall take reasonable precaution to ensure that the coding of health care claims, billings and/or invoices for same are prepared and submitted in an accurate and timely manner and are consistent with federal, state and county laws and regulations.

8.4.2 CONTRACTOR shall not submit any false, fraudulent, inaccurate and/or fictitious claims for payment or reimbursement of any kind.

8.4.3 CONTRACTOR shall bill only for those eligible services actually rendered which are also fully documented. When such services are coded, CONTRACTOR shall use accurate billing codes which accurately describes the services provided and must ensure compliance with all billing and documentation requirements.

8.4.4 CONTRACTOR shall act promptly to investigate and correct any problems or errors in coding of claims and billing, if and when, any such problems or errors are identified.

8.4.5 CONTRACTOR shall promptly return any overpayments within forty-five (45) business days after the overpayment is verified by the HCA.

9. REPORTS

9.1 CONTRACTOR shall:

9.1.1 Submit a complete and accurate bi-weekly CLIENT tracking report to HCA, on a form approved or provided by HCA. The bi-weekly CLIENT tracking report shall include, but is not limited to, data on CLIENTs served and assessment performed by CONTRACTOR in accordance with the services described in Paragraph 11 of Exhibit B to the Agreement.

9.1.2 Provide additional reports as required by HCA in regard to CONTRACTOR's activities as related to the services hereunder. HCA shall be specific as to the nature of information requested and allow thirty (30) calendar days for CONTRACTOR to respond.

9.1.3 Complete reports as required by HCA including bi-weekly CLIENT tracking reports, and Semi-Annual Progress reports.

9.1.4 Comply with data gathering methodology as

prescribed by HCA.

9.1.5 Maintain records, collect data, and provide reports as required by HCA in order to track performance objectives identified in Subparagraph 7 of this Exhibit B to the Agreement.

9.2 CONTRACTOR and HCA may mutually agree to modify the Reports Paragraph 9 of this Exhibit B to the Agreement. Any modification must be in writing.

10. FORMS

HCA will provide a copy of all mandatory State and COUNTY forms. CONTRACTOR shall be responsible for duplication and distribution of the forms to its staff and any subcontractors. CONTRACTOR may develop their own internal forms that are not mandated by COUNTY, or by program requirements. However, internal forms shall be reviewed and approved by HCA prior to implementation.

11. SERVICES

11.1 PERSONS TO BE SERVED

CONTRACTOR shall provide services to eligible CLIENTs regardless of the number, resettled or served by the CONTRACTOR and collaborating RAs, if applicable CLIENTs may include refugees, asylees, Cuban and Haitian entrants, Cuban medical professionals and their spouses and children, certain Amerasians from Vietnam, victims of severe forms of trafficking who receive certification or an eligibility letter from the ORR and certain other specified family members of trafficking victims, and Iraqi and Afghan citizens with Special Immigrant Visa (SIV) status, if deemed eligible by the State of California.

11.2 CONTRACTOR services shall include but not be limited to the following:

11.2.1 Maintain an account in the national Electronic Disease Notification (EDN) system and develop a procedure for identifying entrants. Use EDN to access overseas health examinations, enter tuberculosis

evaluation outcomes for entrants with class B tuberculosis classification, and update information for individuals that move prior to completion of the RHAP assessment, tuberculosis evaluation or completion of treatment for latent tuberculosis infection. HCA shall assist CONTRACTOR in establishing the account.

11.2.2 Maintain an account in the state Refugee Health Electronic Information System (RHEIS), and develop a procedure for data entry of all RHEIS elements. Develop a system to ensure RHEIS is updated in a regular and timely manner (not to exceed ten (10) business days after service or result availability). HCA shall assist CONTRACTOR in establishing the account.

11.2.3 Educate CLIENTs regarding the purpose of the health assessment and the purpose and process for all tests provided during the health assessment.

11.2.4 Complete a comprehensive health assessment for each entrant within ninety (90) days of their US arrival date, date parole status is granted, date asylum status is granted, or date of federal-certification for victims of human trafficking.

11.2.5 Ensure that the health assessments provided include all of the health assessment components as required in the California Refugee Health Assessment Medical Instructions and Form, and Required Medical/Laboratory Evaluation Guidelines.

11.2.6 Assess the immunization status of individuals who have started a health assessment, according to the most current Requirements for Routine Vaccination of Adjustment of Status Applicants, and provide scheduled immunizations or refer individuals to an appropriate provider to receive scheduled immunizations.

11.2.7 Educate individuals regarding conditions found

on the health assessment. Provide medical treatment to individuals identified with a health condition, or refer individuals to an appropriate provider if further medical evaluation is needed.

11.2.8 Evaluate, or refer to an appropriate provider for evaluation, individuals with a positive tuberculosis (TB) skin or blood test for TB infection or disease, and classify according to the most current American Thoracic Society guidelines.

11.2.9 Provide, or refer to an appropriate provider for provision of, treatment of latent TB infection according to the most current CDPH/California TB Controllers Association Joint Guidelines.

11.2.10 If individuals are referred to a health care provider for services, the CONTRACTOR shall develop and document a procedure for staff to follow-up with telephone calls to CLIENTs and providers to document that services were rendered.

11.2.11 Collaborate with the HCA on submission of RHAP grant budget and budget justification, Semi-Annual Progress Report and Final Comprehensive Report.

11.2.12 Develop procedures to carry out policies, and conduct data and medical quality assurance activities to assure staff adherence to policies and procedures.

11.2.13 Provide services in a manner that is culturally and linguistically responsive for the population. CONTRACTOR shall maintain documentation of such efforts which may include, but not be limited to: records of participation in COUNTY-sponsored or other applicable training; recruitment and hiring policies and procedures; copies of literature in multiple languages and formats, as appropriate; and descriptions of measures taken to enhance accessibility for, and sensitivity to, persons who are physically challenged. CONTRACTOR shall provide interpretation during RHAP

health assessment visits and processes, and also to include health education and recommended follow-up for conditions found on RHAP assessments.

11.2.14 CONTRACTOR shall report identified reportable conditions (as per Health and Safety Code Section 2500) to the appropriate unit of COUNTY Public Health Services.

11.3 CONTRACTOR and HCA may mutually agree to modify the Services Paragraph of this Exhibit B to the Agreement. Any modification must be in writing.

12. STAFFING

12.1 CONTRACTOR shall operate continuously throughout the term of this Agreement with at least the minimum number and type of staff which meet applicable federal and state requirements, and which are necessary for the provision of the services hereunder.

12.2 CONTRACTOR shall:

12.2.1 Hire and maintain appropriate staff with the experience and ability to complete all required services in a timely, accurate, and culturally responsive manner.

12.2.2 Have onsite bilingual/bicultural staff to meet the needs of the target population being served. If onsite staff are not available, access to interpretation services are required.

12.2.3 Ensure licensures and/or board certifications for all direct clinical staff allocated to the program are current and in good standing throughout the term of the agreement, and make such documentation available to the County upon request.

12.2.4 Licensed healthcare providers responsible for providing clinical services, including any tests/procedures specific to their licensure specialty, must have at least two (2) years of experience.

12.3 CONTRACTOR shall ensure that its employees, interns, and

volunteers complete the appropriate state mandated trainings prior to service delivery. CONTRACTOR must submit to HCA documents verifying completion of all required training.

12.4 CONTRACTOR and HCA may mutually agree to modify the Staffing section of this Exhibit B to the Agreement. Any modification must be in writing.

12.5 CONTRACTOR shall comply with RHEIS Data Use and Disclosure Agreement requirements, attached herein as Attachment 3 to this Agreement, and ensure that Attachments C and D of Attachment 3 are signed and submitted to COUNTY prior to CONTRACTOR's staff accessing RHEIS.

12.6 CONTRACTOR shall comply with confidentiality requirements as stated in Paragraph 30 of this Agreement when accessing RHEIS. Further, CONTRACTOR shall provide training to staff that uses RHEIS related to the sensitivity of Participant personal information.

13. LITERATURE, ADVERTISEMENTS, AND SOCIAL MEDIA

13.1 Any written information or literature, including educational or promotional materials, distributed by CONTRACTOR to any person or organization for purposes directly or indirectly related to this Agreement must be approved at least thirty (30) days in advance and in writing by HCA before distribution. For the purposes of this Agreement, distribution of written materials shall include, but not be limited to, pamphlets, brochures, flyers, newspaper or magazine ads, and electronic media such as the Internet.

13.2 Any advertisement through radio, television broadcast, or the Internet, for educational or promotional purposes, made by CONTRACTOR for purposes directly or indirectly related to this Agreement must be approved in advance at least thirty (30) days and in writing by HCA.

13.3 If CONTRACTOR uses social media (such as Facebook, Twitter, YouTube or other publicly available social media sites) in support of the

services described within this Agreement, CONTRACTOR shall develop social media policies and procedures and have them available to HCA upon reasonable notice. CONTRACTOR shall inform HCA of all forms of social media used to either directly or indirectly support the services described within this Agreement. CONTRACTOR shall comply with COUNTY Social Media Use Policy and Procedures as they pertain to any social media developed in support of the services described within this Agreement. CONTRACTOR shall also include any required funding statement information on social media when required by HCA.

13.4 Any information as described in Subparagraphs A. and B. shall not imply endorsement by COUNTY, unless HCA consents thereto in writing.

14. HANDLING COMPLAINTS

14.1 CONTRACTOR shall:

14.1.1 Develop, operate and maintain procedures for receiving, investigating and responding to provider and CLIENT complaints, including Civil Rights complaints, requests for reviews by HCA, negative comments and other complaints relating to services provided under this Agreement.

14.1.2 Maintain a log for identification and response to CLIENTs' complaints. When complaints cannot be resolved informally, a system of follow-through shall be instituted which adheres to formal plans for specific actions. Responses to complaints should occur within two (2) business days, unless otherwise authorized by HCA.

14.1.3 For Civil Rights complaints, refer to Subparagraph 8.6.2 of this Agreement.

14.1.4 When CONTRACTOR believes any complaint may have legal implications for CONTRACTOR or COUNTY, CONTRACTOR shall forward such complaint immediately to HCA prior to responding to the complaint. In the event any such complaint pertains to an injury or property damage, CONTRACTOR

shall follow the provisions as set forth in Subparagraph 13.1 of this Agreement.

14.1.5 CONTRACTOR shall provide to HCA, in a form approved by HCA, information pertaining to complaints, as well as CONTRACTOR's response to any complaints as described above within ten (10) business days of the complaint, except as provided in Subparagraph 14.1.4. CONTRACTOR shall provide a summary of all complaints and/or negative comments as prescribed and on a format approved by HCA. Complaints include, but are not limited to, complaints from CLIENTs, other COUNTY contracted service providers, community organizations, and the public.

15. CONTRACTOR STAFF

15.1 Recruitment and Hiring Practices

15.1.1 CONTRACTOR shall use a formal recruitment plan, which complies with Federal and State employment and labor regulations. CONTRACTOR shall hire staff with the education and experience necessary to appropriately perform all functions

15.2 Language Diversity

15.2.1 CONTRACTOR shall employ staff with experience in placing CLIENTs with a limited English vocabulary in an environment that facilitates the development of the English language. CONTRACTOR's staff shall be able to read, write, speak, and understand English. CONTRACTOR shall provide bilingual staff to serve CLIENTs in the language they speak. The ratio of bilingual staff shall be consistent with and proportional to the target population, as determined by HCA. In addition, CONTRACTOR shall be required to provide translation services for all other languages as needed to ensure all participants are provided services in the language they speak.

15.2.2 CONTRACTOR shall comply with all COUNTY, State, and Federal regulations regarding Limited English Proficiency (LEP). LEP

regulations affect anyone who participates in a Federally funded program, and who has English as his or her second language and is limited in his or her English language proficiency.

15.3 Staff Training

15.3.1 CONTRACTOR's staff directly serving CLIENTs/Families, or supervising those who do, shall be thoroughly familiar with RHS rules and California Refugee Health Assessment Medical Instructions and Form, included herein as Attachment 4; HCA policies and related instructions, and child abuse/elder abuse reporting requirements, the State Hearing process, and Civil Rights compliance requirements.

15.3.2 HCA will provide instructions, guidelines, and RHS rules and regulations to CONTRACTOR during start-up, and subsequently as these materials are revised or new policies are developed.

15.3.3 HCA will provide initial training to a limited number of select CONTRACTOR staff with respect to HCA's instructions, guidelines, and RHS rules and regulations; and California Refugee Health Assessment Medical Instructions and Form, CONTRACTOR shall conduct subsequent training(s).

15.3.4 CONTRACTOR shall be required to attend training(s) and/or meetings that HCA determines to be mandatory, and provide CONTRACTOR staff with ongoing training and assistance to ensure that requirements of this Agreement are met. All training materials developed by CONTRACTOR shall be approved by HCA in advance of training.

15.3.5 CONTRACTOR shall ensure that CONTRACTOR staff, as described above, receives training in understanding the cultural differences among groups of CLIENTs, and recognizes and effectively intervenes to overcome any language and/or cultural barriers to employment.

15.3.6 CONTRACTOR shall maintain a log of in-house

training activities and the staff that attended. This log shall be made available to HCA upon request.

16. NOTIFICATION OF DEATH

16.1 Upon becoming aware of the death of any person served pursuant to this Agreement, CONTRACTOR shall immediately notify HCA.

16.2 All Notifications of Death provided to HCA by CONTRACTOR shall contain the name of the deceased, the date and time of death, the nature and circumstances of the death, and the name(s) of CONTRACTOR's officers or employees with knowledge of the incident.

16.2.1 TELEPHONE NOTIFICATION - CONTRACTOR shall notify HCA by telephone immediately upon becoming aware of the death due to non-terminal illness of any person served pursuant to this Agreement; provided, however, weekends and holidays shall not be included for purposes of computing the time within which to give telephone notice and, notwithstanding the time limit herein specified, notice need only be given during normal business hours.

16.2.2 WRITTEN NOTIFICATION

16.2.2.1 NON-TERMINAL ILLNESS - CONTRACTOR shall hand deliver, fax, and/or send via encrypted email to HCA a written report within sixteen (16) hours after becoming aware of the death due to non-terminal illness of any person served pursuant to this Agreement.

16.2.2.2 TERMINAL ILLNESS - CONTRACTOR shall notify HCA by written report hand delivered, faxed, sent via encrypted email, and/or postmarked and sent via U.S. Mail within forty-eight (48) hours of becoming aware of the death due to terminal illness of any person served pursuant to this Agreement.

16.3 If there are any questions regarding the cause of death of any person served pursuant to this Agreement who was diagnosed with a terminal

illness, or if there are any unusual circumstances related to the death, CONTRACTOR shall immediately notify HCA in accordance with this Notification of Death Paragraph.

17. NOTIFICATION OF PUBLIC EVENTS AND MEETINGS

17.1 CONTRACTOR shall notify HCA of any public event or meeting funded in whole or part by the COUNTY, except for those events or meetings that are intended solely to serve CLIENTs or occur in the normal course of business.

17.2 CONTRACTOR shall notify HCA at least thirty (30) business days in advance of any applicable public event or meeting. The notification must include the date, time, duration, location and purpose of public event or meeting. Any promotional materials or event related flyers must be approved by HCA prior to distribution.

18. RECORDS MANAGEMENT AND MAINTENANCE

18.1 CONTRACTOR, its officers, agents, employees and subcontractors shall, throughout the term of this Agreement, prepare, maintain and manage records appropriate to the services provided and in accordance with this Agreement and all applicable requirements.

18.2 CONTRACTOR shall implement and maintain administrative, technical and physical safeguards to ensure the privacy of PHI and prevent the intentional or unintentional use or disclosure of PHI in violation of the HIPAA, federal and state regulations and/or CHPP. CONTRACTOR shall mitigate to the extent practicable, the known harmful effect of any use or disclosure of PHI made in violation of federal or state regulations and/or COUNTY policies.

18.3 CONTRACTOR's participant, CLIENT, and/or patient records shall be maintained in a secure manner. CONTRACTOR shall maintain participant, CLIENT, and/or patient records and must establish and implement written record management procedures.

18.4 CONTRACTOR shall ensure appropriate financial records related to cost reporting, expenditure, revenue, billings, etc., are prepared and maintained accurately and appropriately.

18.5 CONTRACTOR shall ensure all appropriate state and federal standards of documentation, preparation, and confidentiality of records related to participant, client and/or patient records are met at all times CONTRACTOR shall make records pertaining to the costs of services, participant fees, charges, billings, and revenues available within the limits of the County of Orange.

18.6 CONTRACTOR shall ensure all HIPAA (DRS) requirements are met. HIPAA requires that CLIENTs, participants and/or patients be provided the right to access or receive a copy of their DRS and/or request addendum to their records. Title 45 CFR §164.501, defines DRS as a group of records maintained by or for a covered entity that is:

18.6.1 The medical records and billing records about individuals maintained by or for a covered health care provider;

18.6.2 The enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or

18.6.3 Used, in whole or in part, by or for the covered entity to make decisions about individuals.

18.7 CONTRACTOR may retain CLIENT, and/or patient documentation electronically in accordance with the terms of this Agreement and common business practices. If documentation is retained electronically, CONTRACTOR shall, in the event of an audit or site visit:

18.7.1 Have documents readily available within forty-eight (48) hour notice of a scheduled audit or site visit;

18.7.2 Provide auditor or other authorized individuals

access to documents via a computer terminal; or

18.7.3 Provide auditor or other authorized individuals a hardcopy printout of documents, if requested.

18.8 CONTRACTOR shall ensure compliance with requirements pertaining to the privacy and security of PII and/or PHI. CONTRACTOR shall notify COUNTY immediately by telephone call plus email or fax upon the discovery of a Breach of unsecured PHI and/or PII.

18.9 CONTRACTOR may be required to pay any costs associated with a Breach of privacy and/or security of PII and/or PHI, including but not limited to the costs of notification. CONTRACTOR shall pay any and all such costs arising out of a Breach of privacy and/or security of PII and/or PHI.

18.10 CONTRACTOR shall retain all CLIENT, and/or patient medical records for seven (7) years following discharge of the CLIENT and/or patient, with the exception of non-emancipated minors for whom records must be kept for at least one (1) year after such minors have reached the age of eighteen (18) years, or for seven (7) years after the last date of service, whichever is longer.

18.11 CONTRACTOR shall retain all financial records for a minimum of seven (7) years from the commencement of the contract, unless a longer period is required due to legal proceedings such as litigations and/or settlement of claims.

18.12 CONTRACTOR shall make records pertaining to the costs of services, participant fees, charges, billings, and revenues available at one (1) location within the limits of the County of Orange.

18.13 If CONTRACTOR is unable to meet the record location criteria above, HCA may provide written approval to CONTRACTOR to maintain records in a single location, identified by CONTRACTOR.

18.14 CONTRACTOR may be required to retain all records involving litigation proceedings and settlement of claims for a longer term which will

be directed by the HCA.

18.15 CONTRACTOR shall notify HCA of any PRA requests related to, or arising out of, this Agreement, within forty-eight (48) hours. CONTRACTOR shall provide HCA all information that is requested by the PRA request.

19. RESEARCH AND PUBLICATION

CONTRACTOR shall not utilize information and data received from COUNTY or developed as a result of this Agreement for the purpose of personal publication. CONTRACTOR shall not utilize information and/or data received from COUNTY, or arising out of, or developed, as a result of this Agreement for the purpose of personal or professional research, or for publication.

20. RIGHT TO WORK AND MINIMUM WAGE LAWS

20.1 In accordance with the United States Immigration Reform and Control Act of 1986, CONTRACTOR shall require its employees directly or indirectly providing service pursuant to this Agreement, in any manner whatsoever, to verify their identity and eligibility for employment in the United States. CONTRACTOR shall also require and verify that its contractors, subcontractors, or any other persons providing services pursuant to this Agreement, in any manner whatsoever, verify the identity of their employees and their eligibility for employment in the United States.

20.2 Pursuant to the United States of America Fair Labor Standard Act of 1938, as amended, and State of California Labor Code, §1178.5, CONTRACTOR shall pay no less than the greater of the federal or California Minimum Wage to all its employees that directly or indirectly provide services pursuant to this Agreement, in any manner whatsoever. CONTRACTOR shall require and verify that all its contractors or other persons providing services pursuant to this Agreement on behalf of CONTRACTOR also pay their employees no less than the greater of the federal or California Minimum Wage.

20.3 CONTRACTOR shall comply and verify that its contractors comply

with all other federal and State of California laws for minimum wage, overtime pay, record keeping, and child labor standards pursuant to providing services pursuant to this Agreement.

20.4 Notwithstanding the minimum wage requirements provided for in this clause, CONTRACTOR, where applicable, shall comply with the prevailing wage and related requirements, as provided for in accordance with the provisions of Article 2 of Chapter 1, Part 7, Division 2 of the Labor Code of the State of California (§§1770, et seq.), as it exists or may hereafter be amended.

21. SEVERABILITY

21.1 If a court of competent jurisdiction declares any provision of this Agreement or application thereof to any person or circumstances to be invalid or if any provision of this Agreement contravenes any federal, state or county statute, ordinance, or regulation, the remaining provisions of this Agreement or the application thereof shall remain valid, and the remaining provisions of this Agreement shall remain in full force and effect, and to that extent the provisions of this Agreement are severable.

///

///

///

///

///

///

///

///

///

///

///

///

Information Technology Security and Usage

County of Orange Social Services Agency
Administrative Policies and Procedures Manual

Program/Area:	Information Technology				
Title:	Information Technology Security and Usage				
Number:	I 6	**Status:**			Active
Effective Date:	3/20/15	**Date:**		**Revision**	3/16/15

I. PURPOSE

To protect the integrity of the Social Services Agency's (SSA) information technology infrastructure, ensure its availability, reliability, accessibility, and prevent unauthorized disclosure of Confidential Information, including Personally Identifiable Information. Additionally, this policy defines required responsibilities for all users of the SSA information technology infrastructure and supplements the Information Technology Security Policy (ITSP), County of Orange.

II. DEFINITIONS

Confidential Information is defined as information that must be protected from unauthorized disclosure or public release. Examples of Confidential Information include, but are not limited, to the following:

1. Client case records
2. Employment records
3. Payroll and other financial information
4. Other sensitive or business related information that is not intended for wide distribution

Personally Identifiable Information (PII) is information that can be used, alone or in conjunction with any other information, to identify a specific individual. PII includes any information that can be used to search for or identify individuals, or can be used to access their files. Examples of PII may include, but are not limited to: name, SSN, Social Security benefit data, date of birth, official State or government issued driver's license or identification number. PII is a subset of Confidential Information.

SSA workforce members include full-time, part-time and extra-help County of Orange SSA employees, contracted staff, interns, volunteers, and all other authorized individuals with access to SSA's information technology infrastructure.

III. POLICY

SSA workforce members shall adhere to applicable SSA, County of Orange (including the ITSP, County of Orange-Attachment A), State (including the State of California Welfare and Institutions Code 10850), and Federal regulations relating to information technology security, privacy, and confidentiality of information as each may now exist or be herein after amended.

Unless within the scope of job responsibility, any violation of this policy is subject to immediate revocation of user's access to SSA network and associated applications. SSA workforce members may be subject to disciplinary action including suspension, termination, civil, and/or criminal prosecution. Causes for disciplinary action may include, but are not limited, to the following activities:

1. Use of E-mail and all other forms of electronic communication, Internet browsind, or computers, tablets, smart phone and all other electronic devices for any of the following:
   a. Harassing others using offensive, obscene and/or vulgar language; or threatening others, including creating messages containing sexual or
      racial overtones or slurs, and/or messages disparaging of others based on race, sex. age. national origin, sexual orientation, marital status,
      and/or other personal characteristics protected under federal, state or local laws.
   b. Disrupting or interfering with County operations or job responsibilities.
   c. Misrepresenting facts to the detriment of SSA.
2. Unauthorized access to County or other non-County computer networks and/or applications.
3. Failure to protect Confidential Information from unauthorized disclosure.
4. Unauthorized disclosure of Confidential Information.
5. Unauthorized software installation(s) on SSA computer systems.
6. Unauthorized access, attempt to access or to encourage others to access County, State, Federal or other computer systems and networks
   that are not directly within the current scope of employee's job responsibilities.

All SSA workforce members shall do the following:

1. Keep their user IDs and passwords confidential and secured at all times. Should a password be compromised, it shall be changed immediately, and the supervisor shall be notified.
2. Restrict user ID usage only for currently assigned SSA job duties and responsibilities.
3. Use County resources, such as data and information, for County business objectives only. Use of these resources for private or personal gain is prohibited and may be subject to administrative, civil, and criminal penalties (California Penal Code Section 502).
4. Protect Confidential Information of clients to prevent unauthorized disclosure. Only the minimum amount of Confidential Information necessary for business operations should be copied, downloaded, exported or stored on any electronic device or in paper format. Any compromise of Confidential and/or Personably Identifiable Information shall be immediately reported to the supervisor.
5. Request software installations on SSA computers, laptops, tablets and other devices from an authorized agent of the SSA Information Technology team. DO NOT INSTALL ANY software/application into County SSA devices.
6. Seek permission from SSA Information Technology team prior to copying a County-owned software/application.
7. Use of any County electronic communication systems is for business use only; any personal use shall not disrupt or interfere with County operations or job responsibilities.

IV. PROCEDURE

A. The following steps shall be undertaken to ensure that the above policy is enforced to all SSA County employees. Prior to a new employee gaining access to Confidential Information, the SSA Human Resources (HR) representative or designee shall:

1. Provide new employees with access to the SSA I-6 Policy and Procedures document, the ITSP, County of Orange (Attachment A) and the County of Orange Information Technology Usage Policy (Attachment B) with instructions for the new employee to read and sign the SSA Information Technology Security and Usage Agreement (Attachment C). Upon the new employee's signing of SSA Information Technology Usage Agreement form, the HR representative or designee shall counter-sign the completed form.
2. Have the new employee read and sign the Orange County Social Services Agency Confidentiality of Client Information (Attachment D).
3. Confirm that the new employee complete the review of the SSA Information Security Rules of the Road (Attachment E) located in the Training section of the SSA Intranet at http://ocssa/intranet/sites/default/files/Files/administrative/content/I....
4. File the signed SSA Information Technology Usage Agreement (Attachment C), the signed Orange County Social Services Agency Confidentiality of Client Information (Attachment D) and documentation of completion of SSA Information Security Rules of the Road (Attachment E) in the employee's personnel file.

B. The supervisor of an SSA contracted employee, volunteer, intern, and all other non-County employees shall undertake the following steps to ensure that the above policy is enforced. Prior to a workforce member gaining access to Confidential Information, provide them with the following documents to read:

1. Administrative Policies and Procedures Manual I-6 Information Technology Security and Usage;
2. ITSP, County of Orange (Attachment A); and
3. County of Orange Information Technology Usage Policy (Attachment B).

The new workforce member shall document that they have read, understand and will adhere to the policies stated in the SSA I-6 policy and procedures document by signing the document titled: "Agreement to Comply with the Orange County Social Services Agency Information Technology Security and Usage Policy" (Attachment F). This document also includes the SSA Confidentiality Agreement and serves as documentation of completion of the SSA Information Security Rules of the Road training presentation. This action must occur prior to a workforce member being provided with access to Confidential Information.

Maintain this signed "Agreement to Comply with the Orange County Social Services Agency Information Technology Security and Usage Policy" (Attachment F) for three years after the non-County workforce member separates from SSA.
If this workforce member requires access to the SSA network or databases (i.e. shared drives, CalWIN, OnBase, CWS/CMS, SSA Intranet, etc.), a copy of the signed "Agreement to Comply with the Orange County Social Services Agency Information Technology Security and Usage Policy" (Attachment F) shall be provided to SSA IT. Network access will not be provided until this signed document is received.

V. ATTACHMENTS

A. Information Technology Security Policy, County of Orange
B. County of Orange Information Technology Usage Policy
C. SSA Information Technology Security and Usage Agreement
D. Orange County Social Services Agency Confidentiality of Client Information
E. Social Services Agency Information Security Rules of the Road
F. Agreement to Comply with the Orange County Social Services Agency Information Technology Security and Usage Policy

Division:
Administrative

INFORMATION TECHNOLOGY SECURITY POLICY

COUNTY OF ORANGE

Revision History

Date	Revision Scope	Author	Description
12/31/07	All Sections	CEO/IT, ISO	Document creation.
02/21/08	All Sections	CEO/IT, ISO	Document submitted for peer review.
03/10/08	All Sections	CEO/IT	Integration of document revisions.
03/13/08	All Sections	CEO/IT	Integration of document revisions from SWG meeting held 03/13/08.
03/14/08	All Sections	CEO/IT, ISO	Integration of document revisions from meeting with Senior Management held 03/14/08.
03/17/08	All Sections	CEO/IT	Integration of document revisions from SWG meeting held 03/13/08 and HR meeting held 03/17/08.
03/19/08	All Sections	CEO/IT	Integration of document revisions from SWG meeting held 03/18/08.
03/25/08	All Sections	CEO/IT	Integration of document revisions from SWG meeting held 03/13/08, 03/18/08 & 03/24/08; Senior Management meeting held 03/14/08.
04/09/08	Added Appendix, Added Comments	CEO/IT	Added Policy Statement Source Matrix. Added comments for Technology Council Review showing those areas of concern.
06/19/08	Sections 1.3,1.4, 6.2.22	Technology Council	Agency Department Head Signs Approval, forward to CIO for Review and Comment. Use CERT process for Level 4 incident handling.
07/09/08	All Sections	CEO/IT	Corrections to minor typographical/grammatical and formatting errors
07/09/08	Section 2.2.7	CEO/IT	Change requirement that all workforce members read all documents related to County IT security to requirement to read, accept and comply with Workforce Member Usage Agreement.
07/09/08	Section 1.4.1 Section 6.2.18 Section 7.2	CEO/IT	Integration of revisions suggested by SWG Team members.
12/1/08	Section 2.1	CEO/IT	Update to match approved governance diagram
9/15/09	All Sections	CEO/HR	Completed Bargaining unit review and approval

Policy Approval

We have approved this Information Technology Security Policy as reasonably designed to enable the County of Orange and County agencies/departments to address their security obligations for County information assets.

(Signed copy on file in CIO Office)
Satish Ajmani
Deputy CEO/Chief Information Officer

(Signed copy on file in CIO Office)
Tony Lucich
County Information Security Officer

1 INTRODUCTION

Information technology is a critical component of all primary County business processes. The County's visibility on the Internet, the increased use of electronic communication, and a dependence on information technology resources requires the development, maintenance and dissemination of a set of common IT security policies designed to protect these assets.

Security threats, such as identity theft, viruses, and phishing have been increasing both in frequency and in complexity. Due to these increasing security threats, a common set of safeguards is required to minimize the risk, cost and duration of any level of disruption to the County's business processes in the event of damage to or failure, loss, corruption, or discontinuation of a strategic component of its critical IT infrastructure. Ensuring such an environment requires an enterprise approach to security that:

- Promotes an enterprise view among all County agencies/departments
- Recognizes an interdependent relationship among County agencies and/or departments
- Requires adherence to a common, minimum security architecture and related standards, guidelines and procedures

Effective security is a civic responsibility and a team effort involving the participation and support of every County agency, employee and affiliate that deals with information and/or information systems. To further this enterprise-wide responsibility, previously published security-related policies have been consolidated into this IT Security Policy. This document supersedes all prior Countywide IT security polices. This document provides a comprehensive Information Technology Security Policy for County agencies.

It is the responsibility of every County employee and affiliate to know, understand, and adhere to the policy, procedures, standards, and guidelines contained herein and to conduct their activities accordingly. This policy statement has been adopted in order to provide guidance and protection to County employees and to safeguard the information resources entrusted to those employees. Information security policies raise user awareness of the potential risks associated with information technology. Employee awareness through dissemination of policy helps minimize the cost of security incidents; accelerate the development of new application systems; and assure the consistent implementation of controls for information systems throughout the organization.

County information security policy is based upon the ISO 27002:2005 standards, the NIST standards, and Best Practices. The policy is designed to comply with applicable laws and regulations; however, if there is a conflict, applicable laws and regulations will take precedence. The policy statements are to be considered minimum requirements for providing a secure environment for the development, implementation, and support of information technology and systems. Agencies may develop detailed policies and procedures to handle agency-specific cases.

The enterprise security policy and standards established under the authority described herein are resources intended to assist County agencies and/or departments to more effectively manage the information technology resources.

1.1 AUTHORITY

The authority to set technology policy for all agencies is derived from the County IT Strategic Plan. The IT Security Policy was developed in conjunction with the security guiding principles along with the governance and compliance goals set forth in the County IT Strategic Plan. The IT Governance Model, discussed below, executes this plan by facilitating change agreement for the IT Security Policy. The County IT Strategic Plan states *"The County will adhere to an agreed-upon minimum set of security/privacy controls."* as this supports countywide strategic priorities. Supporting the foundational principle of *"driving towards the use of common IT components"*, the County IT Strategic Plan states *"The County will have an agreed-upon baseline set of security monitoring and incident response policies."*

1.2 IT GOVERNANCE MODEL

IT governance consists of leadership, stakeholder engagement, and collaboration processes that ensure that the County's IT investments support overall business strategies and policy objectives. IT governance facilitates general agreement on IT policies, resources, and architecture.

The Technology Council receives input from multiple Architecture Groups and Working Groups, including the Technology Architecture Group (TAG) and the Security Working Group (SWG). Changes or updates to this policy may be proposed by any Architecture Group or Working Group. The SWG works collaboratively with the ISO to make recommendations to the Technology Council and the Business Council through the governance process. The SWG also advises the office of the CIO and Technology Council as appropriate. As needed, proposals will be forwarded to the Technology Council and Business Council for review and approval. The Technology Council is responsible for reviewing and recommending IT guiding principles, standards, policies, and guidelines to the CIO. The Business Council is responsible for approving IT guiding principles, standards, policies, and guidelines proposed by the CIO and/or Technology Council.

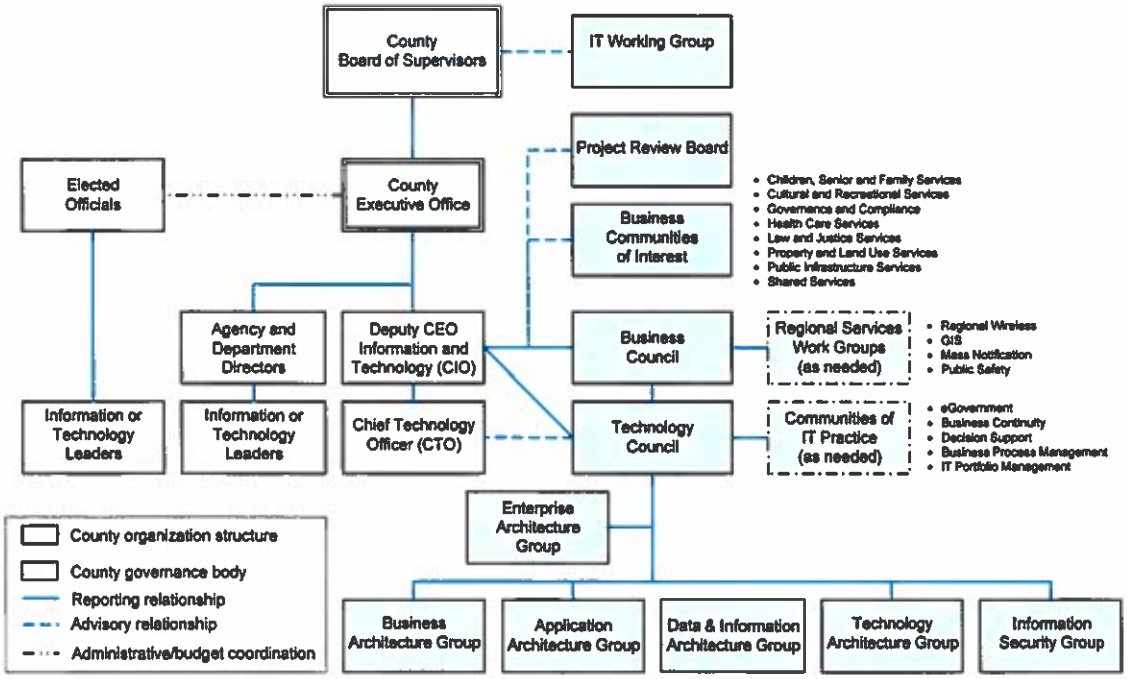

Fig. 1: **County IT Governance Model**

1.3 ENFORCEMENT

Individual County agencies and/or departments will be responsible for developing an IT Security Plan including detailed procedures to comply with this policy. Each agency IT Manager will create a Security Plan based on this framework guideline that this meets the intent and submit to their Agency Director for signature approval. Agencies will submit their approved IT Security Plans to the CIO for review and comment. (Please see Exceptions section for more information.)

The IT Security Policy will guide periodic security reviews as well as audits by the Internal Audit Department. In addition, the County will review applicable equipment and service purchases to ensure that vendors and contractors are aware of policy and are in compliance with it. Violators of policy may be subject to employee disciplinary procedures. Agencies may impose sanctions upon their employees for violations of policy and standards. All disciplinary actions and/or sections must be in compliance with applicable Human Resources policy.

1.4 EXCEPTIONS

Agencies will document the need for exceptions to this policy, including the scope and extent of the exception; the safeguards to be implemented to mitigate risks; the specific timeframe for the exception; and evidence of management approval of the exception.

The policy described in this document is applicable to production-level systems. Internal test and experimental systems not connected to a production network do not require the same level of security unless they make use of confidential information.

Application development systems may also be exempt provided they are on a network that is physically separated or suitably isolated from production networks. However, if development or test systems are on the same physical or virtual network as production systems or contain confidential information, they must follow the same security policy as production systems.

1.4.1 HIPAA

While they address similar topics, the County Health Insurance Portability and Accountability Act (HIPAA) Policies and the IT Security Policy function as separate policies. The IT Security Policy is more comprehensive in scope as compared with the HIPAA Policy. The HIPAA Policy establishes County policy pursuant to federal HIPAA security requirements for use of electronic protected health information (ePHI) by the County and designated health care entities.

ePHI is also addressed within the IT Security Policy. If a conflict exists between this policy and the HIPAA Policy, the HIPAA Policy will prevail. The County HIPAA Security Policy is available at:
http://intra2k3.ocgov.com/cota/policies/brd_of_supervisors.asp

1.5 IT SECURITY PROGRAM IMPLEMENTATION PROCESS

The County Board of Supervisors approved the CIO to develop a comprehensive security program. This security program is based on the County IT Strategic Plan. The following diagram illustrates the process being used to define and implement the County's information security program.

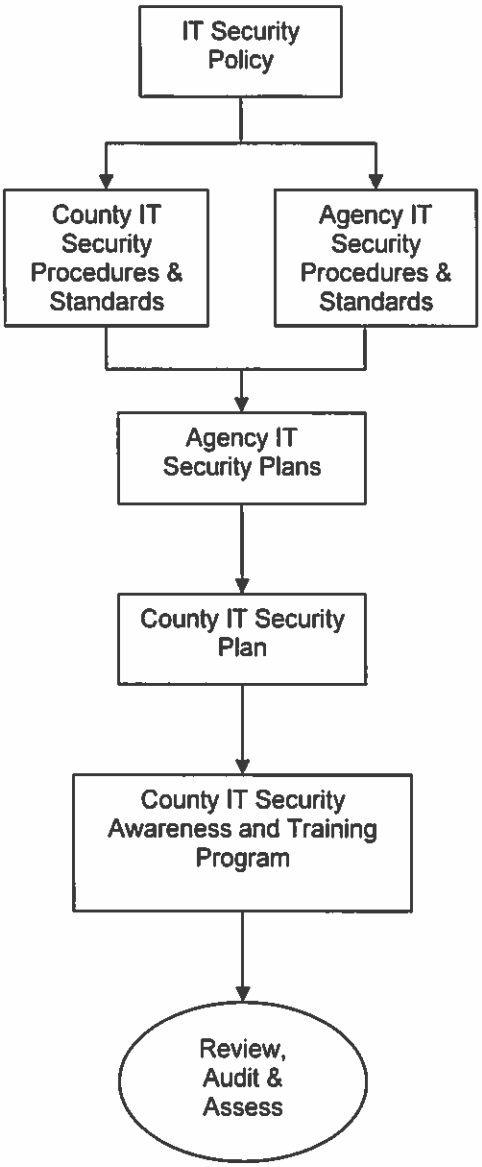

Fig. 2: **County IT Security Program Implementation Process**

1.6 SCOPE/LIMITATIONS

This policy applies to all agencies in the County as well as all employees, contractors, vendors, customers, and others who utilize, possess or have access to County IT resources.

2 INFORMATION TECHNOLOGY SECURITY

2.1 PURPOSE

The purpose of this document is to define a common security environment within the County to:

- Foster system security and availability
- Ensure data integrity and confidentiality, and
- Encourage the prevention of unauthorized access or damage to, or misuse or loss of, County IT assets and/or data

2.2 POLICY STATEMENT

2.2.1 All information that is created or used within the County's trusted environment in support of County business activities shall be considered the property of the County. All County property should be used in compliance with the IT Security Policy.

2.2.2 County information is a valuable asset and must be protected from unauthorized disclosure, modification, or destruction. Prudent information security standards and practices must be implemented to ensure that the integrity, confidentiality, and availability of County information are not compromised. All County information shall be protected from the time of its creation through its useful life and authorized disposal.

2.2.3 The County shall be responsible for the policy defined in this document. An independent annual review of County Information Security control objectives, policy and procedures shall be completed by a resource identified by the Chief Information Officer (CIO).

2.2.4 County information technology resources are provided to authorized users to facilitate the efficient and effective performance of their duties. The use of such resources imposes certain responsibilities and obligations on users and is subject to County policy and applicable state and federal laws. It is the responsibility of users to ensure that resources are not misused and that they comply with policy.

2.2.5 This policy provides a minimal security framework for the County and each individual agency. In the event that an agency does not have or maintain its own IT security policy, the agency should, at a minimum, adopt and adhere to this policy.

2.2.6 Agencies contracting with business partners, such as contractors, consultants or vendors, shall use IT policy guidelines provided and approved by the CIO and County Council (COCO) to ensure the safeguarding of County information systems. These contracts must be reviewed for appropriate compliance with County Business Continuity and IT Security Policies.

2.2.7 Each agency shall ensure that all County workforce members within its organization read, accept and comply with the IT Security Policy Workforce Member Usage Agreement.

2.2.8 Each agency shall ensure that all software used on County systems and in the execution of County business shall be used legally and in compliance with licensing agreements.

2.2.9 Each agency shall ensure that all County workforce members within its organization, including employees, contractors, and consultants, receive appropriate training in IT security. IT security training is to be conducted on an annual basis.

2.3 RELATED POLICY

- Agency policy as applicable.

3 ORGANIZATIONAL SECURITY

3.1 PURPOSE

Organizational Security is intended to facilitate information security within an organization through the implementation of an information security infrastructure. An information security infrastructure is the complete set of information security-related systems, procedures, policies and physical implementations of information security administration.

Organizational Security specifically applies to any situation in which a County agency uses resources from a vendor or contractor to access and perform work with County information systems.

3.2 POLICY STATEMENT

3.2.1 The primary function of the Security Working Group (SWG) is to bring together representatives from different parts of the organization with relevant security roles and job functions for the purpose of collaboratively establishing information security strategies for selected IT initiatives. The SWG advises the office of the CIO and the Technology Council as appropriate.

3.2.2 Each agency should identify an Information Security Officer (ISO), responsible for management of information security issues for that agency. Each agency decides which appropriate qualifications and criteria are to be used for selection of an ISO.

3.2.3 All agencies should clearly define information security responsibilities in the following areas (at a minimum):

- Information Security Management
- Information Classification
- Risk Assessment
- Compliance
- Business Continuity/Disaster Recovery
- Software Development Oversight
- Incident Response
- Security Awareness/Training.

3.2.4 All agencies shall consult with the ISO when developing new information processing facilities, applications and access methods to ensure consistency with existing and anticipated IT security policies.

3.2.5 Employees who need to access confidential information are required to sign confidentiality and/or non-disclosure agreements when initially hired. External users (contractors, vendors and customers) who are not already covered by an existing agreement should also sign such agreements prior to being given access to confidential information. Confidentiality and non-disclosure agreements should be reviewed regularly, especially when employees leave the organization or when contracts expire.

3.2.6 Risk assessment and identification should take place prior to establishing vendor, customer or contractor access to County information systems and must be in accordance with the policy set forth in this document (see Section 7: Access Control).

3.2.7 Contractors and vendors who have access to Personal Identifiable Information, as defined herein, shall comply with the California Information Practices Act and the Consumer Credit Reporting Act, as applicable.

3.2.8 Any agreement or contract with a vendor, contractor or customer that involves access to County information resources will contain sections that delineate County information security issues relevant to that business access and require the vendor, contractor and/or customer to adhere to County IT Security Policy. If Security is outsourced, the vendor must demonstrate a standard of care as this must also be reflected in the vendor contract.

3.2.9 The office of the CIO shall make experienced resources available to agencies to complete annual reviews of the agency's approach to managing information security and its implementation (e.g. objectives, controls, policies, processes and procedures).

4 HUMAN RESOURCES SECURITY

4.1 PURPOSE

Human Resources Security addresses information security throughout the entire lifecycle of employment, from the recruitment stage, during an individual's employment, and through termination or separation. County workforce members include all employees, contractors, vendors and customers working to forward the County's mission.

Some of the specific purposes of Human Resources Security are to:

- Minimize the risks at the recruitment stage of employment for all potential County workforce members
- Ensure that County workforce members are knowledgeable and aware of security threats, concerns, and the procedures for reporting security incidents
- Ensure that a disciplinary process is in place to deter County workforce members who may disregard security policy and procedures

4.2 POLICY STATEMENT

4.2.1 Based on an employee's role and job responsibilities, agencies must conduct personnel screenings/background checks of prospective employees who will be granted access to County information systems.

4.2.2 All agencies should use terms and conditions of employment to clearly state the employee's responsibilities for information security. Such terms and conditions are typically defined in a non-disclosure or confidentiality agreement that is signed by the employee and maintained by Human Resources. The agreement should also define actions that will be taken in the event of non-compliance.

4.2.3 County and agency-specific disciplinary procedures will be followed for users who disregard security policies, standards and procedures.

4.2.4 Upon termination, separation or applicable job change (including but not limited to moves, adds, transfers, promotions, change of duties, and change in job responsibilities):

- Employee must return all County assets
- Human Resources must notify appropriate IT personnel to update and/or remove employee access rights
- An exit interview is to be conducted and must include confirmation that all necessary assets and access (both physical and logical) have been returned to the County

4.2.5 Human Resources will provide a list of terminated employees and employee changes to IT on a quarterly basis. Human Resources is responsible for reviewing inactive/unused user account reports as provided by IT and providing updates to IT as appropriate.

4.2.6 Agencies contracting with business partners, such as contractors, consultants or vendors, shall ensure that personnel screenings/background checks are addressed as part of the business relationship.

4.3 RELATED POLICY

- Sections 2.2.10-2.2.12: Security Awareness
- Section 3.2.5: Non-disclosure/Confidentiality Agreements

5 PHYSICAL AND ENVIRONMENTAL SECURITY

5.1 PURPOSE

Physical and Environmental Security is intended to protect County assets from harm caused by physical threats (e.g., civil unrest, sabotage, assault) or environmental events (e.g., earthquake, flood, fire, severe weather). Physical and environmental security measures are used in conjunction with the County Business Continuity Management Policy to protect County assets.

Specific areas addressed in this section are:

- Physical safeguards to the perimeter of agency facilities
- Prevention of unauthorized physical access
- Reduction in risk from environmental threats and hazards
- Protection of business critical equipment and information systems from power anomalies
- Protection of sensitive information assets from improper data cleansing and disposal

5.2 POLICY STATEMENT

5.2.1 Procedures and facility hardening measures shall be adopted to prevent attempts at and detection of unauthorized access or damage to facilities that contain County information systems and/or processing facilities.

5.2.2 Restricted areas within facilities that house sensitive or critical County information systems will, at a minimum, utilize physical access controls designed to permit access by authorized personnel only.

5.2.3 Physical protection measures against damage from external and environmental threats shall be implemented by all agencies as appropriate.

5.2.4 Access to any office, computer room, or work area that contains sensitive information shall be physically restricted from unauthorized access.

5.2.5 Access points such as delivery and loading areas and other points where unauthorized persons may enter the premises shall be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access. An example of this would be separating the two areas by a badge-only accessible door.

5.2.6 Continuity of power should be provided to maintain the availability of critical equipment and information systems.

5.2.7 Power and telecommunications cabling carrying data or supporting information services should be protected from interception or damage. Different, yet appropriate methods should be utilized for internal and external cabling.

5.2.8 Equipment should be properly maintained to ensure its continued availability and integrity.

5.2.9 Unless approved by County management, no County computer equipment should be removed from the premises.

5.2.10 Prior to re-deployment, surplus, donation, disposal or destruction of equipment containing storage media, media should be appropriately cleansed to prevent unauthorized exposure of data. NIST standards should be followed for appropriate levels of storage media cleansing.

5.2.11 Disposal of equipment shall be done in accordance with all applicable County, state or federal surplus property and environmental disposal laws, regulations or policies.

5.2.12 All shared IT infrastructure by more than one agency shall meet countywide security policy for facility standards, availability, access, data & network security.

5.3 RELATED POLICY

- County Business Continuity Management Policy

6 SYSTEM AND NETWORK OPERATIONS MANAGEMENT

6.1 PURPOSE

System and Network Operations Management includes the documentation and maintenance of operating procedures to ensure the secure operation of information processing facilities for the County. The existence of standard operating procedures reduces organizational dependence upon individual and institutional knowledge. The process of creating standard operating procedures requires detailed examination of process activities, the reason behind them and, in relevant cases, how the process could be improved.

System and Network Operations Management addresses the following areas:

- Implementation of formal change management control procedures
- Separation of development, testing, and operational computing environments
- Reduction in the risk of exposure when external contractors provide information processing facilities for County systems or services
- Proper management of capacity planning
- Reduction of the risk of system failure due to inadequate testing and validation
- Prevention and detection of malicious software
- Routine data backups and storage
- Preparation and testing of procedures and facilities for restoration of backup data
- Logging and reporting of all services, activity and faults
- Protection of connected services from unauthorized access and the security of data on networks
- Security of all County operational system documentation
- Creation of software exchange agreements
- Electronic data interchange involving various forms of commerce
- Establishment and use of email systems
- Internet Usage
- Use of publicly available methods of access (e.g., the Internet) to County information resources

6.2 POLICY STATEMENT

6.2.1 Operating procedures and responsibilities for all County information processing facilities should be formally authorized, documented, and maintained.

6.2.2 Changes to all information processing facilities, systems, software, or procedures should be strictly controlled according to formal change management procedures.

6.2.2.1 Unauthorized users should not make any changes to system and/or software configuration files.

6.2.2.2 Unauthorized users should not download and/or install operating system software, service-related software (such as web server software), or other software applications on County computer systems without prior written authorization from agency IT management. This includes, but is

not limited to, free software, computer games and peer-to-peer file sharing software.

6.2.2.3 Each agency should develop a formal change control procedure that outlines the process to be used for identifying, classifying, approving, implementing, testing, and documenting changes to its IT resources.

6.2.2.4 Each agency should conduct periodic audits designed to determine if unauthorized software has been installed on any of its computers.

6.2.3 As appropriate, segregation of duties should be implemented by all County agencies to ensure that no single person has control of multiple critical systems and the potential for misusing that control.

6.2.4 Production computing environments should be separated from development and test computing environments to reduce the risk of one environment adversely affecting another.

6.2.5 System capacity requirements should be monitored and usage projected to ensure the continual availability of adequate processing power, bandwidth, and storage.

6.2.6 System acceptance criteria for all new information systems and system upgrades must be defined, documented, and utilized to minimize risk of system failure.

6.2.7 Security awareness, prevention, and detection controls should be utilized to protect information systems and services against malicious software and against the unauthorized execution of mobile code (e.g., ActiveX controls, Java applets).

6.2.8 Backups of all essential electronically-maintained County business data should be routinely created and properly stored to ensure prompt restoration.

6.2.8.1 Each agency should implement and document a backup approach for ensuring the availability of critical application databases, system configuration files, and/or any other electronic information critical to maintaining normal business operations within the agency.

6.2.8.2 The frequency and extent of backups should be in accordance with the importance of the information and the acceptable risk as determined by each agency.

6.2.8.3 Agencies should ensure that locations where backup media are stored are safe, secure, and protected from environmental hazards. Access to backup media should be commensurate with the highest level of information stored and physical access controls should meet or exceed the physical access controls of the data's source systems.

6.2.8.4 Backup media should be labeled and handled in accordance with the highest sensitivity level of the information stored on the media.

6.2.8.5 Agencies should define and periodically test a formal procedure designed to verify the success of the backup process.

6.2.8.6 Restoration from backups should be tested initially once the process is in place and periodically afterwards. Confirmation of business functionality after restoration should also be tested in conjunction with the backup procedure test.

6.2.8.7 The system backup schedule should be published for users and is intended to ensure that users are aware of the procedures for the established backup process.

6.2.8.8 Agencies should retain backup information only as long as needed to carry out the purpose for which the data was collected, or for the minimum period required by law.

6.2.9 Systems operational staff should maintain appropriate log(s) of activities, exceptions and information security events involving County information systems and services.

6.2.10 Each agency should maintain a log of all faults involving County information systems and services.

6.2.11 Agencies should establish controls to ensure the security of the information systems networks that they operate.

6.2.12 When no longer required, the contents of removable media should be permanently destroyed or rendered unrecoverable in accordance with applicable agency, County, state, or federal record disposal and/or retention requirements.

6.2.13 Agencies should establish internal procedures for the secure handling and storage of all electronically-maintained County information that is owned or controlled by the agency.

6.2.14 Operational system documentation for County information systems should be protected from unauthorized access.

6.2.15 Agreements should be implemented for the exchange of information between the County and other entities.

6.2.16 County information accessed via electronic commerce should have security controls implemented based on the assessed risk.

6.2.17 Electronic mail should be governed for acceptable use and shall be open to inspection or review by management to comply with County, state and federal laws and regulations as well as any applicable agency policies. The use of email for conducting County business should be based on business management decisions regarding the appropriateness of the medium.

6.2.17.1 The email system and network are primarily for official business only.

6.2.17.2 County or agency authorization for an individual to use encryption or other measures to protect or "lock" email messages shall not constitute consent by the County or agency to maintain any such message as private.

6.2.17.3 Each user of a County email system shall have an individual email account that is uniquely linked to that user. General purpose email accounts, however, may be used for departmental interaction between the public and County employees (e.g., the general email account webmaster@ocgov.com is used to communicate with the general public).

6.2.17.4 Users should not use an internal County email account assigned to another individual to send or receive messages.

6.2.17.5 Use of Internet (external) email systems from County networks and/or desktop devices is prohibited unless there is a compelling business reason for such use.

6.2.17.6 Users shall not configure or use automated forwarding of County email messages to Internet (external) email systems unless specifically authorized to do so with written authorization by County management.

6.2.17.7 Confidential or restricted documents sent as attachments to email messages shall be treated as confidential or restricted documents. These same restrictions shall apply to confidential or restricted information embedded within an email message as message text.

6.2.17.8 If a business need exists to communicate confidential information within the County it may be done so by email with permission of management by sending the email only to those who have a need to know the information and by marking it "CONFIDENTIAL."

6.2.17.9 Using email to communicate confidential information should be the exception, not the rule. Memoranda and reports on paper, telephone calls, and face-to-face meetings should be used in specific contexts (e.g., the communication of personnel matters).

6.2.17.10 Special features designed to filter out malicious software contained in either email messages or email attachments should be implemented on all County email systems.

6.2.17.11 Users should not delete email messages whose subject matter has been identified as relevant to pending or anticipated litigation or other legal processes.

6.2.17.12 Agencies will provide their users with training on the appropriate use of both the Internet and County email systems and on the handling of email messages and attachments.

6.2.18 The Internet/Intranet access is primarily for official business only. County workforce members may access the Internet for limited personal business only during nonworking time and in strict compliance with the other terms of this policy. If there is any doubt about whether a contemplated activity is appropriate for County business purposes, employees may consult with their immediate supervisor to help decide if a use is appropriate.

6.2.18.1 In order to control Internet content that is seen by County workforce members, Agencies may use Web-filtering or content-control software.

6.2.18.2 In order to monitor, track and log Internet sites visited during normal work hours, Agencies may monitor, track, log and report on County workforce members Internet traffic.

6.2.19 Public access to County electronic information resources should provide desired services in accordance with safeguards designed to protect County resources.

6.2.20 The clocks of all relevant information processing systems should be synchronized with an agreed upon accurate time source such as an established Network Time Protocol (NTP) service.

6.2.21 County issued rules for use and maintenance of computers and other equipment include:

- Liquids or magnets are not to be kept on or near computers, as these can cause serious damage
- All original software assigned to County workforce members must be available when the system needs to be serviced in case the software needs to be reinstalled
- When a computer problem is discovered, all details about the problem should be recorded/communicated on the appropriate form and/or when called into Service Desk or discussed with IT staff.
- Equipment should be plugged into a surge protector at all times
- Any damage to equipment is to be reported to the appropriate authorities

The County may, on occasion, issue additional rules concerning the use and maintenance of computers and other equipment.

6.2.22 County Agencies are responsible for establishing internal processes to ensure vulnerability management. This includes the efficient application of vendor-supplied patches or other mitigations based on the following levels of criticality. The related applications should be tested pre and post patch deployment.

- Level 1 – Maintenance: Patches addressing non-security related issues are to be applied at agency/department discretion
- Level 2 – Required: Patches addressing theoretical security vulnerabilities are to be applied within two weeks of notification of patch availability
- Level 3 – Mandatory: Patches addressing security vulnerabilities for which an exploit exists are to be applied within one week of notification of patch availability
- Level 4 – Urgent: Patches addressing security vulnerabilities currently being exploited by Internet attacks are to be applied within 48 hours of notification of patch availability. Level 4 urgent patches shall to use the Incident Process and Management portion of this Policy. Notification of patch status is to be sent to CEO/IT.

6.2.23 Security vulnerability management policy applies to routers, switches, servers, desktops and laptops owned by the County, whether located on the County's internal network, another facility or in the offsite possession of a County employee, contractor, vendor or customer. This also applies to any contractor, vendor or customer owned equipment connected to the County network.

6.3 RELATED POLICY

- Section 9: Information Security Incident Management

7 ACCESS CONTROL

7.1 PURPOSE

Access Control is defined to ensure only authorized access to County information systems and resources with the overarching goal of protecting the confidentiality, integrity, and availability of all County resources. Information access and County computing processes should be controlled on the basis of County business and applicable security policies.

Access Control addresses the following areas:

- Allocation of user access rights
- Management of user access privileges
- Prevention of the assignment of unauthorized access privileges
- Establishment of a standard for password controls
- Reinforcement of the use of effective passwords
- Guidelines for access and use of networks and networked services
- Guidelines for the use of wireless network access technology
- Guidelines for activity timeout procedures for any networked session
- Appropriate system utilities access
- Establishment of valid logon connection schedules
- Disclosure of unauthorized activity through the use of monitoring activity and tracking logs
- Prevention of system security compromises during the use of mobile computing devices
- Guidelines on security issues involved in remote access

7.2 POLICY STATEMENT

7.2.1 GENERAL ACCESS

7.2.1.1 Agencies should establish a procedure that ensures only users with legitimate business needs to access County IT resources are provided with user accounts.

7.2.1.1.1 Access to County information systems and information systems will be based on each user's access privileges. Access controls must ensure that even legitimate users cannot access stored information unless they are authorized to do so.

7.2.1.1.2 The owner of each non-public County system, or their designee, provides written authorization for all internal and external user access.

7.2.1.1.3 All access to internal County computer systems shall be controlled by an authentication method involving a minimum of a user identifier (ID) and password combination that provides verification of the user's identity.

7.2.1.1.4 All County workforce members are to be assigned a unique user ID to access the network.

7.2.1.1.5 A user account should be explicitly assigned to a single, named individual. No group or shared computer accounts are permissible except when necessary and warranted due to legitimate business needs. Such need must be documented prior to account creation and accounts activated only when necessary.

7.2.1.1.6 User accounts should not be shared with others including, but not limited to, someone whose access has been denied or terminated. If the person using another person's account violates this policy by using that account, it is considered to be the same as the original account owner violating policy. Both persons are then subject to the consequences of that violation.

7.2.1.1.7 By accepting account passwords and other information from the County and accessing the network or the Internet, County workforce members are agreeing to follow the IT Security policy.

7.2.1.1.8 County approved password standards and/or guidelines should be applied to the access of all County systems.

7.2.1.1.9 Passwords are a primary means to control access to systems and should therefore be selected, used, and managed to protect against unauthorized discovery or usage. (e.g., use passwords of eight or more characters, including at least one number and one uppercase character).

7.2.1.1.10 Passwo rd management systems should be deployed where feasible to comply with the County Single Sign-On Initiative.

7.2.1.1.11 Periodic log reviews of user access and privileges should be performed in order to monitor access of sensitive information.

7.2.1.1.12 Auditing and logging of user activity should be implemented on all critical County systems that support user access capabilities.

7.2.1.1.13 All workforce members are responsible for creating and maintaining the confidentiality of the password associated with their unique user ID. Upon receipt of a user ID, the person assigned the user ID is required to change the temporary password provided by the administrator to a password known only to the user.

7.2.1.1.14 Ne wly-created accounts should be assigned a randomly-generated password prior to account information being provided to the user.

7.2.1.1.15 No user shall give his or her password to another person under any circumstances. Workforce members who suspect that their password has become known by another person

shall change their password immediately and report their suspicion to management in accordance with Section 9: Incident Management.

7.2.1.1.16 Users who have lost or forgotten their passwords must make any password reset requests themselves without using a proxy (e.g., another County employee) unless approved by management. Prior to processing password change requests, the requester must be authenticated to the user account in question. (e.g. Verification with user's supervisor or the use of passphrases can be used for this authentication process.) New passwords should be provided directly and only to the user in question.

7.2.1.1.17 Agenci es should require workforce members to change their network and application passwords periodically (e.g., every 90 days at the maximum). Changing passwords more often than 90 days is encouraged.

7.2.1.1.18 Whe n technologically feasible, network and application systems should be configured to enforce automatic expiration of passwords at regular intervals (e.g., every 90 days at the maximum).

7.2.1.1.19 When technologically feasible, a new or reset password shall be set to expire on its initial use at log on so that the user is required to change the provided password to one known only to them.

7.2.1.1.20 All privileged system-level passwords (e.g., root, enable, OS admin, application administration accounts, etc.) should be changed at least every 90 days.

7.2.1.1.21 All passwords are to be treated as sensitive and highly confidential information.

7.2.1.1.22 At the time of network login, the user shall be presented with a County Council-approved statement ("login banner") containing language regarding the appropriate use of computer systems.

7.2.1.1.23 Employees may be asked from time-to-time to provide new or additional registration and account information, for example, to reflect developments in the law or technology. Employees must provide this information if they wish to continue to receive service. If after employees have provided their account information, some or all of the information changes, employees must notify the person designated by the County to receive this information.

7.2.1.2 Automated screen lockouts should be used wherever possible using a set time increment (e.g., 15 minutes of non-activity). In situations where it is not possible to automate a lockout, operational procedures should be implemented to instruct users to lock the terminal or equipment so that unauthorized individuals cannot make use of the system. Once logged on, workforce members should normally not leave their computer unattended or available for someone else to use.

7.2.1.3 Access to a the County network and its resources should be strictly controlled, managed, and reviewed to ensure only authorized users gain access based on the privileges granted. (e.g., Kiosks provide physical and public access to County networks. These should be secured to ensure County resources are not accessed by unauthorized users.)

7.2.1.4 The control mechanisms for all types of access to County IT resources by contractors, customers or vendors are to be documented.

7.2.1.5 System utilities should be available to only those users who have a business case for accessing the specific utility.

7.2.1.6 All applications are to have access controls unless specifically designated as a public access resource.

7.2.1.7 When deemed necessary, user logins and data communications may be restricted by time and date configurations that limit when connections will be accepted.

7.2.1.8 The decision to use cryptographic controls and/or data encryption on a hard drive should be based on the level of risk of unauthorized access and the sensitivity of the data that is to be protected.

7.2.2 COUNTY WIRELESS ACCESS

7.2.2.1 Agencies shall take appropriate steps, including the implementation of appropriate encryption, user authentication, device authentication and malware protection measures, to mitigate risks to the security of County data and information systems associated with the use of wireless network access technologies.

7.2.2.1.1 Only wireless systems that have been evaluated for security by both agency management and by the CIO should be approved for connectivity to County networks.

7.2.2.1.2 County data that is transmitted over any wireless network must be protected.

7.2.3 NON-COUNTY ACCESS

7.2.3.1 All access to County networks or resources via unapproved wireless communication technologies is prohibited. This includes wireless systems that may be brought into County facilities by visitors or guests. Employees, contractors, vendors and customers are prohibited from connecting and/or activating wireless connections on any computing device that are simultaneously connected to any County network, either locally or remotely.

7.2.3.2 Each agency should make a regular, routine effort to ensure that unauthorized wireless networks, access points, and/or modems are not installed or configured within its IT environments. Any unauthorized connections described above should be disabled immediately.

7.2.3.3 All remote access implementations that involve non-County infrastructures should be reviewed and approved by both the agency ISO and the CIO or their designee. This approval should be received prior to

the start of such implementation. The approval should be developed as a memorandum of understanding (MOU).

7.2.3.4 Any computing device, including laptops and desktop PCs, that has been connected to a non-County infrastructure (including employee home networks) and subsequently used to connect to the County network should be verified that it is free from viruses and other forms of malicious software prior to attaining connectivity to the County network.

7.2.3.5 Remote access privileges to County IT resources should not be given to contractors, customers or vendors unless agency management determines that these individuals or organizations have a legitimate business need for such access. If such access is granted, it should be limited to those privileges and conditions required for the performance of the specified work.

7.2.4 REMOTE ACCESS

7.2.4.1 Agencies shall take appropriate steps, including the implementation of appropriate encryption, user authentication, and virus protection measures, to mitigate security risks associated with allowing users to use remote access or mobile computing methods to access County information systems.

7.2.4.1.1 Remote access privileges should be granted to County workforce members only for legitimate business needs and with the specific approval of agency management.

7.2.4.1.2 All remote access implementations that utilize the County's trusted network environment and that have not been previously deployed within the County should be submitted to and reviewed by the CIO's office. A memorandum of understanding (MOU) should be utilized for this submittal and review process.

7.2.4.1.3 Session inactivity timeouts should be implemented for all remote access into and from County networks.

7.2.4.1.4 All remote access infrastructures must include the capability to monitor and record a detailed audit trail of each remote access attempt.

7.2.4.1.5 All users of County networks and computer systems are prohibited from connecting and/or activating unauthorized dial-up or broadband modems on workstations, laptops, or other computing devices that are simultaneously connected to any County network.

7.2.4.1.6 Each agency will conduct regular internal audits in order to identify unauthorized remote connections.

7.2.4.1.7 Users granted remote access to County IT infrastructure must follow all additional policies, guidelines and standards related to authentication and authorization as if they were connected locally. For example, this applies when mapping to shared network drives.

7.2.4.1.8 Users attempting to use external remote access must utilize a County-approved multi-factor authentication process.

8 SYSTEMS DEVELOPMENT AND MAINTENANCE

8.1 PURPOSE

The integration of security measures with systems development, customization, and maintenance activities ensures that business applications, mission-critical software and commercial off-the-shelf software (COTS) do not become a security threat to the organization's assets. County applications, mission-critical software and COTS should be implemented and maintained in a safe and effective manner. If there is a conflict between Federal and State owned or controlled systems and this policy, the Federal and State owned or controlled systems prevail over this policy.

System Development and Maintenance addresses:

- Security related business requirements for new systems or enhancements to existing systems
- Controls for integration into applications to ensure that each level or type of information access is secure at a consistent level
- Controls on data input, output, access and processing
- Cryptographic security controls for new systems or enhancements to existing systems
- Securing operating system files and application software
- Securing system test data
- Securing access to program source libraries
- Change controls for systems development and maintenance
- Change or upgrade processes for production operating systems
- Purchased software and changes to executable code provided by a vendor
- Avoiding unauthorized introduction of unintentional and intentional malicious software

8.2 POLICY STATEMENT

8.2.1 GENERAL

8.2.1.1 Agencies should identify all business applications that are used by their users in support of primary business functions. This includes all applications owned and/or managed by the agency as well as other business applications that are used by the agency but owned and/or managed by other County organizations. All business applications used by an agency should be documented in the agency's IT security plan as well as their Business Impact Analysis (BIA).

8.2.1.2 An application owner should be designated for each internal agency business application.

8.2.1.3 All access controls associated with business applications should be commensurate with the highest level of data used within the application. These same access controls should also adhere to the policy provided in Section 7: Access Control.

8.2.1.4 Security requirements should be incorporated into the evaluation process for all commercial software products that are intended to be used as the

basis for a business application. The security requirements in question should be based on requirements and standards specified in this policy

8.2.1.5 In situations where data needs to be isolated because there would be a conflict of interest (e.g., DA and OCPD data cannot be shared), data security will be designed and implemented to ensure that isolation.

8.2.2 REQUI REMENTS

8.2.2.1 The business requirements definition phase of system development must contain a review to ensure that the system will adhere to County information security standards.

8.2.3 CORRECT PROCESSING OF APPLICATIONS

8.2.3.1 Owners of IT systems should implement checks on data input to ensure the data is correct and appropriate. An example of this is utilizing input checks to detect: out-of-range values, invalid characters, missing or incomplete data, and data exceeding upper or lower volume limits or unauthorized or inconsistent control data.

8.2.3.2 Owners of IT systems should use validation checks within applications to detect any corruption of information through processing errors or deliberate acts. An example of this is the use of appropriate programs to recover from a failure to ensure the correct processing of data.

8.2.3.3 Owners of IT systems should ensure the authentication of all messages sent and received within those systems. An example of this is using cryptographic techniques to authenticate messages containing confidential or sensitive information.

8.2.3.4 Data output from an application should be validated to ensure that the processing of stored information is correct and appropriate to the business transaction. An example of this is using reconciliation control counts to ensure processing of all data.

8.2.4 CRYPT OGRPAHIC CONTROLS

8.2.4.1 The decision to use cryptographic controls and/or data encryption in an application should be based on the level of risk of unauthorized access and the sensitivity of the data that is to be protected.

8.2.4.1.1 Where appropriate, encryption should be used to protect confidential or restricted application data that is transmitted over open, untrusted networks, such as the Internet.

8.2.4.1.2 Whe n cryptographic controls are used, procedures addressing the following areas should be established by each agency:

- Determination of the level of cryptographic controls
- Key management/distribution steps and responsibilities

8.2.4.1.3 Encryption keys should be exchanged only using secure methods of communication.

8.2.4.1.4 To ensure interoperability, encryption technologies should be based on the architecture standards established by the CIO.

8.2.5 SYSTEM FILES

8.2.5.1 Operating system files, application software and data should be secured from unauthorized use or access.

8.2.5.2 Clear-text data that results from testing should be handled, stored, and disposed of in the same manner and using the same procedures as are used for production data.

8.2.5.2.1 System tests should be performed on data that is constructed specifically for that purpose.

8.2.5.2.2 System testing should not be performed on operational data unless the necessary safeguards are in place.

8.2.5.3 A combination of technical, procedural and physical safeguards should be used to protect application source code from unintentional or unauthorized modification or destruction. All County proprietary information, including source code, needs to be protected through appropriate role-based access controls. An example of this is a change control tool that records all changes to source code including new development, updates, and deletions, along with check-in and check-out information.

8.2.6 SYSTEM DEVELOPMENT & MAINTENANCE

8.2.6.1 Policies established by this IT Security Policy will be incorporated into the system development of new business applications that are developed internally or that are developed for County or agency use by vendors, contractors or consultants.

8.2.6.2 The development of software for use on County information systems must have documented change control procedures in place to ensure proper versioning and implementation.

8.2.6.3 When preparing to upgrade any County information systems, including an operating system, on a production computing resource; the process of testing and approving the upgrade should be completed in advance in order to minimize potential security risks and disruptions to the production environment.

8.2.6.4 Systems should be hardened and logs monitored to ensure the avoidance of the introduction and exploitation of malicious code.

8.2.6.4.1 All County workforce members shall not create, execute, forward, or introduce computer code designed to self-replicate, damage, or impede the performance of a computer's memory, storage, operating system, or application software.

8.2.6.5 In conjunction with other access control policies, any opportunity for information leakage should be prevented through good system design practices.

8.2.6.6 Agenci es are responsible for monitoring outsourced software development related to agency-owned IT systems.

8.3 RELATED POLICY

- Section 7: Access Control.
- Sections 6.2.2 – 6.2.2.4: Change Control information

9 INFORMATION SECURITY INCIDENT MANAGEMENT

9.1 PURPOSE

Information Security Incident Management establishes the policy to be used by each agency in planning for, reporting on, and responding to computer security incidents. For these purposes an incident is defined as any irregular or adverse event that occurs on a County system or network.

9.2 POLICY STATEMENT

9.2.1 Security incident management procedures should be established within each agency to ensure quick, orderly, and effective responses to security incidents.

The steps involved in managing a security incident are typically categorized into six stages:

- System preparation
- Problem identification
- Problem containment
- Problem eradication
- Incident recovery
- Lesso ns learned

9.2.1.1 Agencies should document procedures for reporting security incidents through appropriate management channels.

9.2.1.2 Agencies should document procedures for intrusion detection.

9.2.2 Agencies should establish procedures to enable the types, volumes, and costs of information security incidents to be quantified and monitored.

9.2.3 Where a follow-up action against an entity after an information security incident will involve civil or criminal legal action, evidence should be collected, retained, and presented to conform to the rules for evidence as demanded by the relevant jurisdiction(s). At the Agency's discretion, they may obtain the services of qualified external professionals to complete these tasks.

9.2.4 Each agency should designate one individual as its Information Security Officer (ISO). The ISO will act as the liaison between applicable parties during a security incident. The ISO will be a member of the Information Security Team (IST) as well as the agency's primary point of contact for all IT security issues. The agency ISO should designate an alternate contact to act as the liaison should s/he be unavailable.

9.2.4.1 A directory or phone tree should be created listing all agency security incident liaison contact information.

9.2.4.2 Each agency shall train its employees on the use of its security incident reporting procedures.

9.2.5 Each agency shall develop a procedure for users to report perceived threats to the security of information systems. For example, all employees, contractors, vendors and customers of County information systems should be required to note and report

any observed or suspected security weaknesses in systems to management. In the event an agency has not established these procedures, the County ISO may be contacted for assistance.

9.2.6 Agencies will respond to security advisory information received from either internal (e.g., County) or approved external sources by promptly undertaking appropriate and/or recommended procedures intended to mitigate the effects of actual or potential security incidents.

9.2.7 Contact with local authorities, including law enforcement, shall be conducted through an organized, repeatable process that is both well documented and communicated.

9.2.8 Contact with special interest groups, including media and labor relations, shall be conducted through an organized, repeatable process that is both well documented and communicated.

10 BUSINESS CONTINUITY AND DISASTER RECOVERY

10.1 PURPOSE

Business Continuity is intended to counteract interruptions in business activities and to protect critical business processes from the effects of significant disruptions. Disaster Recovery provides for the restoration of critical County assets, including IT infrastructure and systems, staff, and facilities.

10.2 POLICY STATEMENT

10.2.1 Each agency shall develop, periodically update, and regularly test business continuity and disaster recovery plans in accordance with the County's Business Continuity Management Policy.

10.2.2 Agencies will, at a minimum, review and update their Risk Assessments (RAs) and Business Impact Analyses (BIAs) on an annual basis. As detailed in Section 12: Risk Assessment and Treatment, RAs include agency identification of risks that can cause interruptions to business processes along with the probability and impact of such interruptions and the consequences to information security. A BIA establishes the list of processes and systems that the agency has deemed critical after performing a risk analysis.

10.2.3 Continuity plans should be developed and implemented to provide for continuity of business operations in the event that critical IT assets become unavailable. Plans must provide for the availability of information at the required level and within the established Recovery Time Objective (RTO)

10.2.4 Each agency should maintain a comprehensive plan document containing its business continuity plans. Plans should be consistent, address information security requirements, and identify priorities for testing and maintenance. Plans should be prepared in accordance with the standards established by the County's Business Continuity Management Policy.

10.3 RELATED POLICY

- County Business Continuity Management Policy
- Section 12: Risk Assessment and Treatment

11 COMPLIANCE

11.1 PURPOSE

Compliance establishes the operation of County information systems in accordance with applicable law; statutory, regulatory or contractual obligations; and security requirements.

11.2 POLICY STATEMENT

11.2.1 The County Information Security Policy must comply with state and federal regulations all well as identify the relevant statutory and regulatory requirements.

11.2.2 Each agency should implement appropriate procedures to ensure compliance with state and federal regulations on the use of intellectual property.

11.2.3 Each agency should acquire software only through known and reputable sources to ensure that software licensing and copyrights are not violated.

11.2.4 Agency management should ensure that all security procedures within their area of responsibility are carried out correctly to achieve compliance with security policies and standards.

11.2.5 Agencies should periodically review written procedures and information systems to ensure ongoing compliance with security policies and applicable standards.

11.2.6 Agencies should develop formal IT audit policy and procedures. Audit policy and procedures should address the following:

- The type of processes to be audited
- Use of read-only access to data to conduct the audit
- Planning for audits on operational systems to minimize the risk of disruptions to business processes.
- Avoiding conflicts of interest by putting in place an independent auditor (i.e., someone who does not participate in the activities being audited)
- Protection of information systems audit tools to prevent any possible misuse or compromise.

11.2.7 The use of the network and Internet is a privilege, not a right. If policy is violated, the offender may be subject to termination of network and/or Internet access. The County may refuse to reinstate such access for the remainder of the offender's tenure at the County. The County may also take other disciplinary action as allowed under County policy. A violation of this policy may also be a violation of the law and subject the user to investigation and criminal or civil prosecution.

11.3 RELATED POLICY

11.3.1 Section 2: Information Technology Security

12 RISK ASSESSMENT AND MITIGATION

12.1 PURPOSE

Risk assessments should identify, quantify, and prioritize risks against County assets, systems, processes and deliverables. The results should guide and determine the priorities for information security risk management and for implementing controls selected to protect against risks. Mitigation of risks furthers the County's goal of protecting its assets from harm.

12.2 POLICY STATEMENT

12.2.1 Agencies should develop and implement risk assessment policies based on Best Practices that should include the systematic approach of estimating the magnitude of risks (risk analysis) and the process of comparing the estimated risks against risk criteria to determine the significance of the risks (risk evaluation).

12.2.2 Agencies should perform the process of assessing risks and selecting the controls for coverage of multiple organizational information assets or individual information systems.

12.2.3 Risk assessments should be performed periodically to address changes in the security requirements and in the risk situation, e.g., changes in assets, threats, vulnerabilities, impacts, or risk evaluation methodologies and when significant infrastructure changes occur. These risk assessments should be undertaken in a methodical manner capable of producing reproducible results.

12.2.4 Before considering risk mitigation, the agency should decide criteria for determining whether or not risks can be accepted. Risks may be accepted if, for example, it is assessed that the risk is low or that the cost of mitigation is not cost-effective for the agency.

12.2.5 For each of the risks identified following the risk assessment, a risk mitigation decision needs to be made. Possible options for risk mitigation include:

- Risk Limitation - applying appropriate controls to reduce the risks
- Risk Assumption - knowingly and objectively accepting risks, providing such acceptance satisfies the organization's policy and criteria for risk acceptance
- Risk Avoidance - avoiding risks by not allowing actions that would cause the risks to occur
- Risk Transference - transferring the associated risks to other parties, e.g., insurers or suppliers

12.2.6 For those risks where the risk mitigation decision has been to apply appropriate controls, these controls should be selected and implemented to meet the requirements identified by the risk assessment. Controls should ensure that risks are reduced to an acceptable level, taking into account:

- Requirements and constraints of County, state and federal legislation and regulations
- Orga nizational objectives
- Operational requirements and constraints

- Cost of implementation and operation in relation to the risks being reduced and keeping mitigation costs proportional to the organization's requirements and constraints
- Need to balance the investment in implementation and operation of controls against the harm likely to result from security failures

12.3 RELATED POLICY

- Business Continuity Management Policy

13 PRIVACY

13.1 PURPOSE

Personal Identifiable Information (PII) should be protected from unauthorized use. The unauthorized use of PII is the leading cause of identity theft; specifically national identification numbers or Social Security Numbers.

13.2 POLICY STATEMENT

13.2.1 All County workforce members with access to PII shall treat information as confidential and take all secure precautions necessary to ensure this information is not compromised. The accidental or intentional disclosure of PII to unauthorized users is in violation of this policy.

13.2.2 All information created, sent, or received via the email system, network, Internet, telephones or the Intranet is the property of the County. Employees should not have any expectation of privacy regarding such information. This includes all email messages and electronic files. The County reserves the right to, at any time and without notice, access, read and review, monitor, and copy all messages and files on its computer system as it deems necessary. When it believes necessary, the County may disclose text or images to law enforcement without the employee's consent.

13.2.3 All hardcopy or printed materials containing PII shall be treated as confidential information. This should not be left unattended for any period of time. This information should be physically destroyed by an approved process before discarding it.

14 APPENDIX A: DEFINITIONS

The following definitions apply to all policies presented in this document, as well as to all other documents developed as part of the County's IT Security efforts.

*For purposes of this document, the following three terms are to be interpreted as the definitions indicate.

> *Must:* This word, or the term "SHALL", mean that the policy is an obligation.
>
> *Shall:* must; is or are obliged to
>
> *Should:* This word means that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.

ALPHABETICAL LISTING (A – Z)

Agency/Department: Any reference to "agency" or "department" refers to County agencies, departments, and/or County managed organizations that operate within the trusted environment.

Application Owner: A designated individual within an agency who is responsible for defining and enforcing the application's operating parameters, authorized functions, and security requirements.

Authentication: Process during which valid users are uniquely identified, and their identification is verified, prior to being given access to County information assets.

Authorization: Following authentication, the level of privileges that are assigned to individual users of IT resources.

Authorized: To have been granted officially sanctioned and accurate access to an IT resource.

Backup: The process of copying/duplicating files, databases, and/or system files to avoid loss of data and to facilitate recovery in the event of a system problem or failure.

Business Continuity: The ability of an organization to provide service and support for its customers and to maintain its viability before, during, and after a business disruption.

Business Continuity Plan: Management approved document that defines the arrangements and procedures that enable an organization to respond to an event that lasts for an unacceptable period of time and to return to performing its critical business functions after an interruption.

CERT: Computer Emergency Response Team

Change Control: A combination of technical, physical, and procedural safeguards used to protect systems and/or software applications from unintentional and/or unauthorized modification.

CIO: Chief Information Officer for the County

Clear-text data: data stored or transferred without cryptographic protection

Compliance: Conformation to local, state, and federal laws and to the IT Security Policy set forth by the County.

Confidentiality/Non-Disclosure Agreement: An agreement between at least two parties that outlines confidential materials or knowledge the parties wish to share with one another for certain purposes, but wish to restrict from generalized use. The parties agree not to disclose information covered by the agreement.

Contractor: A temporary non-employee conducting authorized business within County resources via access rights similar to those of County employees. For these purposes, "consultant" is synonymous with "contractor".

County (of Orange): For the purposes of this document, any reference to "County" is to be interpreted as "County of Orange".

County ISO: The County Executive Office Information Security Officer.

County Workforce Members: All employees, contractors, vendors and customers working to forward the County's mission.

Cryptographic Controls: Controls used to secure County information resources, such as data encryption, digital signatures, non-repudiation services, and key management.

Customer: Anyone who receives services from the County.

DAD: Director of Application Development.

Data/Information: Any communication or information, including but not limited to numeric, graphic, or narrative information, maintained on any medium including, but not limited to, computerized databases, paper, microform, optical/magnetic disk, magnetic tape, and/or in transit over a communications network. No distinction is made between the word "data" and "information" for purposes of the IT Security Policy.

Development Oversight: Review of software and application development for security risks. This includes Software Quality Assurance (SQA) techniques.

Disaster: A sudden, unplanned catastrophic event causing unacceptable damage or loss. (1) An event that compromises an organization's ability to provide critical functions, processes, or services for some unacceptable period of time. (2) An event where an organization's management invokes its recovery plans.

Disaster Recovery: The ability of an organization to respond to a disaster or an interruption in services by implementing a disaster recovery plan to stabilize and restore the organization's critical functions.

Disaster Recovery Plan: Management approved document that defines the processes, resources, actions, tasks and data required to manage technology and infrastructure recovery efforts. This is a component of the Business Continuity Management Program.

DSO: Director of Systems Operations.

Encryption: The process of transforming information (referred to as "plaintext") using an algorithm (a "cipher") to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key.

> *Algorithm (Encryption):* A set of ordered steps for solving a problem, such as a mathematical formula or the instructions in a program. This is used in conjunction with a key to encrypt or decrypt information.

Data (Encryption): The process and result of using encryption on electronic information (data) to secure it from unauthorized access.

Data at Rest (Encryption): Encryption of data that is located in a single location, such as a hard drive or tape storage.

Data in Transit (Encryption): Encryption of data that is transmitted from point A to point B. Data in transit encryption can be performed via email; XML at the application layer; or in network packets at the data link, network or transport layers.

Key: A secret numeric code that is used to encrypt text for security purposes.

Key Management (Encryption): The secure creation, management, storage and use of encryption keys.

Key Distribution (Encryption): The secure distribution and exchange of encryption keys between parties using encrypted communication. This includes how keys are made available to both parties. For example, using asymmetric encryption requires the use of public keys that could be stored on a public directory website.

Enterprise: The entire County and its attendant entities, including all agencies and departments that operate within the trusted environment. The enterprise excludes special districts such as OCTA, Law Library, and the Cemetery District.

Environmental Threat: Any threat to County operations that is manifested via the environment including, but not limited to, fire, flood/water damage, earthquake, severe weather, and airborne toxins.

External Threat: Any threat to County operations that is manifested from outside the County enterprise.

Guidelines: A guideline is similar to a standard or policy in that it outlines a specific principle, direction, directive, specification, or procedure. Unlike a standard or policy, a guideline is not binding but is instead a recommended course of action.

IID (Internal Intrusion Detection): Detection of an intrusion generated by misuse or attempted misuse of organizational resources by legitimate users.

Incident: The term incident in this document is defined as any irregular or adverse event that occurs on a County system or network. Examples of incidents include:

- Loss of service, equipment or facilities
- System malfunctions or overloads
- Huma n errors
- Non-compliances with policies
- Breaches of physical security
- Unplanned or unauthorized system changes
- Malfunctions of software or hardware
- Acce ss violations

Incident Response: The process of formally acting and reporting on an incident that has been identified to the Incident Management Team, the Information Security Officer, or appropriate management.

Information Classification: The labeling of information assets according to their sensitivity to disclosure. Label include *Confidential, Sensitive, Restricted* and *Public.*

Information Processing Facilities: A physical or logical entity that is used in the processing of information within the scope of the County. Examples include a complete data center, a new database application or a single laptop.

Information Security Infrastructure: The complete set of information security-related systems, procedures, policies and physical implementations of information security administration.

Information Security Management: Management of all agency-related information security issues including: (1) Formulation, review and approval of agency information security policy; (2) Maintenance of threat assessments for internal information; (3) Oversight of investigations into security-related incidents; and (4) Oversight of business issues regarding new security initiatives.

Information Security Team: The Information Security Team (IST) is an Agency-defined team that will act as the incident coordination team for all Agency-related security incidents. An example of a team framework includes the SA, DSO, DAD, and Departmental CIO.

Information Systems: Any combination of computer hardware and software that generates, processes, transmits, accepts, and/or stores data or information.

Information Systems Application / Business Application: Any software program that has been developed, acquired, or modified specifically to support a unique and identifiable County business function. This includes applications used across multiple agencies and/or departments.

IT Security Policy: A general or high level statement of a direction, purpose, and principle for managing and protecting technology and technology resources.

Local Security Administrator: Resource identified within each agency that is responsible for the operational maintenance of IT security resources within the agency.

Loss of Data: The unforeseen loss of data or information.

Misuse: Any use of information, systems and resources that is out of compliance or is in conflict with County policies, applicable state and federal laws and/or County IT Security Policy.

Mobile Computing: Any computing device that can be disconnected from one network and re-attached to another network. This includes portable devices such as notebook computers, Personal Digital Assistants (PDAs), smart phones, pocket PCs and Lo-jack or other real-time tracking devices. This also includes desktop PCs in those circumstances where the desktop device is disconnected from one network and then reconnected to another network. Since wireless access devices work in this manner, they are also considered to be mobile computers for the purposes of this policy.

Non-County Infrastructure: Any network or environment in which the device(s) and/or network equipment are not under the direct control and management of designated County IT network support staff. This includes, but is not limited to, vendor facilities, other government facilities, employee homes, the Internet, and devices in County facilities that are not directly connected to the County's network.

NTP (Network Time Protocol): A mechanism for synchronizing the clocks of computer systems over packet-switched data networks.

Offender: Someone who violates County policy or any local, state, or federal law or regulation.

Operational System Documentation: Operational manuals, tables, access control lists, or other documentation that contain sensitive information which, if divulged, could compromise the security of

the systems referenced within such documentation. (e.g., network diagrams, router configurations, firewall rule sets, etc.)

Personal Identifiable Information (PII): any piece of information that can potentially be used to uniquely identify, contact, or locate a single person. Examples include full name, national identification number, driver's license number, etc.

Personnel Screening/Background Check: Use of a defined, repeatable process to verify a person's background. An example includes a system such as LiveScan.

Physical Threat: Any threat to County operations that is manifested physically. Examples include civil unrest, physical sabotage, and physical assault of facilities.

Procedures: Specific steps, tasks, and activities to be performed to implement IT security policy. As a general rule, agencies and/or departments are responsible for establishing procedures that adhere to the County IT Security Policy.

Remote Access: Any access of County IT assets from a non-County infrastructure (including employee homes), no matter what technology is used to gain access.

Risk Assessment: The process by which risks are identified and the impact of those risks determined.

SA: Security Administrator.

Security Awareness/Training: The process of educating all County users about the IT Security Policy and/or all appropriate agency Information Security Policies.

Security Plan: In the context of the County IT Strategic Plan and this document, the security plan includes security policy, procedures and standards. The County is developing a security plan including this security policy with procedures/standards to follow. Agencies will also develop security plans including an Agency security policy, procedures and standards.

Security Working Group: A committee assembled from security resources throughout the County. Its primary function is to discuss security issues and technologies and to create security policies and guidelines for use by all County agencies and departments.

Standards: A prescribed or proscribed specification, approach, directive, procedure, solution, methodology, product or protocol that must be followed in order to comply with the IT Security Policy.

Systems Development: The process by which an information systems application is created and deployed. This general term is used to describe the entire lifecycle of a new County application, including requirements gathering, coding, testing, implementation and deployment, and retirement.

System Hardening: The process of eliminating or minimizing vulnerabilities on a computer system. Techniques used include anti-virus software; firewalls; configuration changes to remove unused access points (e.g., email, web and FTP servers/ports); and patch level maintenance.

Systems Maintenance: The process of updating existing County information system applications, including application and/or operating system code and configuration changes.

Theft: The illegal taking of another's property without that person's freely given consent.

Trusted Environment: An information system and network or combination of systems/networks that is under the direct control and management of County personnel.

Written Authorization: Methods include email, memo, letter, security access change form, and change in active directory or user account database.

Users: Any reference to "users" should be interpreted as individuals accessing and/or using County IT assets, including full or part-time employees, contractors, consultants, interns, volunteers, and any other authorized individuals attempting access or use of the County's IT infrastructure.

Vault: A double-locking manhole cover that prevents unauthorized access from the street level.

Vendor: Any entity that sells or provides services to the County.

15 APPENDIX B: IT ETIQUETTE

All users must abide by rules of network etiquette, which include being polite and using the network and the Internet in a safe and legal manner.

16 APPENDIX C: PROHIBITED ACTIVITY

The County or authorized County officials will make a good faith judgment as to which materials, files, information, software, communications, and other content and activities are permitted and prohibited based on the following guidelines and under particular circumstances.

Unless workforce members are specifically authorized due to their work assignment, the following are among uses that are considered unacceptable and constitute a violation of this policy:

(a) Using, transmitting, or seeking inappropriate or offensive materials, including vulgar, profane, suggestive, obscene, abusive, harassing, belligerent, threatening, or defamatory (harming another's reputation by lies) language or materials.

(b) Revealing PII without permission, such as another's home address, telephone number, credit card number or Social Security Number.

(c) Making offensive or harassing statements or jokes about language, race, color, religion, national origin, veteran status, ancestry, disability, age, sex, or sexual orientation.

(d) Sending or soliciting sexually oriented messages or images.

(e) Visiting sites featuring pornography, terrorism, espionage, theft, drugs or other subjects that violate or encourage violation of the law.

(f) Gambling or engaging in any other activity in violation of local, state, or federal law.

(g) Uses or activities that violate the law or County policy or encourage others to violate the law or County policy. These include:

- Without proper authorization, accessing, transmitting, or seeking confidential information about clients or coworkers
- Conducting unauthorized business
- Intruding, or trying to intrude, into the folders, files, work, networks, or computers of others, or intercepting communications intended for others
- Knowingly downloading or transmitting confidential information

(h) Uses that cause harm to others or damage to their property. These includes:

- Downloading or transmitting copyrighted materials without the permission of the copyright owner. Even if materials on the network or the Internet are not marked with the copyright symbol, ©, one should assume that they are protected under copyright laws unless there is explicit permission stated concerning their use
- Using another's password or other user identifier that misleads message recipients into believing that someone other than the authenticated user is communicating or otherwise using the other's access to the network or the Internet
- Intentionally uploading a virus, other harmful component, or corrupted data or vandalizing any part of the network
- Using any software on the network other than that licensed or approved by the County.

(i) Uses that jeopardize the security of and access to the County network or other networks on the Internet

(j) Accessing, attempting to access, or encouraging others to access controversial or offensive materials. Be advised that access to the network and the Internet may include the potential for access to materials inappropriate for use in County business, including materials that may be illegal, defamatory, or offensive. Certain of these areas on the Internet may contain warnings as to their content and users are advised to heed these warnings. Not all sites that may contain inappropriate material, however, will include warnings. Responsibility must be taken for use of the network and the Internet and these sites must be avoided.

(k) Commercial uses. Do not:

- Buy or sell anything over the Internet
- Solicit or advertise the sale of any goods or services (whether to one recipient or many, such as "junk e-mail")
- Use County information technology for unauthorized outside fund-raising activities, participating in any lobbying activity, or engaging in any prohibited partisan political activity
- Use County information technology to post County, department and/or other public agency information to external news agencies, service bureaus, bulletin boards or other forums except with prior authorization

(l) Uses that waste limited resources. For example:

- Printing of personal files, which wastes toner or paper in printers.
- Chain letters, even for noncommercial or apparently "harmless" purposes, as these, like email with large graphic attachments and "junk e-mail," use limited network resources.
- Including unnecessary recipients on an email. Only copy others on an email who should be "in the loop" on the topic addressed.
- Indiscriminate use of distribution lists. Before using a distribution list, determine whether or not it is appropriate for everyone on that list to receive the email.
- "All hands" emails. Emails of this type are to be sent only after management permission has been obtained.

17 APPENDIX D: RESPONSIBILITIES

17.1 INFORMATION TECHNOLOGY SECURITY

17.1.1 Agency management has the ultimate responsibility for ensuring that all individuals within their organizations understand and comply with the IT Security Policy.

17.1.2 All users with either direct or indirect access to County information systems are responsible for understanding and complying with the IT Security Policy as well as any additional policies or procedures mandated by the individual agencies.

17.2 ORGANIZATIONAL SECURITY

17.2.1 The County is responsible for providing a basic security infrastructure framework to be used by all agencies and/or departments within the County. Where agency business need exceeds the County-provided security infrastructure, the agency is responsible for working collaboratively with CEO/IT to determine and implement a solution.

17.2.2 All persons that engage the services of or work with contractors, vendors or customers are responsible for understanding and adhering to organizational security policy.

17.3 HUMAN RESOURCES SECURITY

17.3.1 Agency management is responsible for following this policy and for ensuring their employees follow this policy.

17.3.2 Agency management is responsible for conducting disciplinary procedures as appropriate.

17.3.3 Agency management is responsible for initiating changes to access rights. The local security administrators are responsible for processing these requests and confirming their completion with the requesting manager or supervisor.

17.3.4 A County workforce member's responsibility for information security should be reviewed annually.

17.4 PHYSICAL AND ENVIRONMENTAL SECURITY

17.4.1 All County agencies that house information processing facilities are responsible for implementing procedures to follow the physical and environmental security policy, including identifying the perimeter of the facility and performing a risk analysis to assess its physical security.

17.4.2 All County employees, contractors, vendors and customers are required to adhere to the physical and environmental security policies established by the authorized agency.

17.5 SYSTEM AND NETWORK OPERATIONS MANAGEMENT

17.5.1 The Local Security Administrator, in conjunction with the agency director and the agency ISO, is responsible for implementing procedures to follow the operations and communications security policy listed in this document.

17.5.2 Each system administrator is responsible for providing a quarterly report to agency management listing all unaccessed user accounts. Upon the completed review of this report, system administrators are to take appropriate action as directed by agency management.

17.5.3 All County employees, contractors, vendors and customers that work in an operational and communication role are required to adhere to the operations and communications security procedures established by the related agency.

17.5.4 CEO/IT is responsible for the assignment of patch criticality levels. Criticality levels will be assigned based upon notification from DHS, InfraGard, SANS or Security Focus. CEO/IT is further responsible for the publication of patch availability notifications as well as for policy compliance tracking and reporting.

17.6 ACCESS CONTROL

17.6.1 All County workforce members are required to adhere to the access control procedures established by the related agency.

17.6.2 Agency management is responsible for ensuring their staff adheres to access control policy listed above.

17.6.3 All system administrators are responsible to provide the password for a new unique user ID to only the user to whom the new ID is assigned. When a password reset is requested by a user, the system administrator is responsible for verifying the identity of the user or verifying that the person making the request is authorized to request a password reset for another user.

17.7 SYSTEMS DEVELOPMENT AND MAINTENANCE

17.7.1 Users are to be held responsible for all activities that occur while using their assigned application accounts.

17.7.2 Agencies are responsible for monitoring all security-related changes in law and regulations as well as any other legal requirements that may impact the security of a business application. Agencies/departments are to ensure that any required modifications to support legal and regulatory requirements are implemented in a timely manner.

17.7.3 Developers and Users should only use application accounts appropriate to their level of access.

17.8 INCIDENT MANAGEMENT

17.8.1 Each Agency is responsible for fully cooperating in the County's security incident response policy as well as in a common, countywide process designed to mitigate the effects of security incidents.

17.8.2 The IST is involved in the investigation of any Agency-based security incident. The IST is responsible for assigning personnel to specific incident response tasks and for coordinating the overall incident response. In some events, directives given by a member of the IST will supersede this document.

17.8.3 Agency IT staff is responsible for routinely evaluating system logs and other pertinent information for signs of security incidents and for periodically checking security advisory listings and other sources of security alert information.

17.8.4 It is the responsibility of each employee, contractor, vendor, and customer to safeguard information and to report breeches or threats to all County information processing systems.

17.8.5 It is the responsibility of CEO/IT to provide Agencies with incident escalation procedures.

17.9 BUSINESS CONTINUITY AND DISASTER RECOVERY

17.9.1 Agencies are ultimately responsible for development, maintenance, testing and implementation of their respective business continuity and disaster recovery plans.

17.10 COMPLIANCE

17.10.1 Agency management is responsible for ensuring that agency activities are in compliance with the IT Security Policy

17.11 RISK ASSESSMENT AND MITIGATION

17.11.1 The agency identified ISO is responsible for their agency's security programs, including risk management. They play a leading role in introducing an appropriate, structured methodology to identify, evaluate, and minimize risks to the agency.

17.11.2 Local Security Administrators (LSA) are responsible for proper implementation of security requirements on their local IT systems. As those systems change through expansion, maintenance and upgrades, the LSA must support and use the risk assessment and mitigation process to address new security risks and implement new security controls as needed.

17.11.3 System and information owners are responsible for ensuring that proper controls are in place to address the integrity, confidentiality, and availability of the IT systems and data they own. System and information owners are responsible for changes to their IT systems. The system and information owners must therefore understand their role in the risk management process and fully support this process by working with the agency ISO and LSA.

17.12 PRIVACY

17.12.1 All County workforce members are responsible for the security of PII.

18 APPENDIX E: POLICY STATEMENT SOURCES

Policy Section	Source Title	Source Section
1	ISO/IEC 2005:27002	06.1.1 Management commitment to information security
2.2	ISO/IEC 2005:27002	05.1.1: Information Security Policy document
2.2.3	ISO/IEC 2005:27002	05.1.2 Review of the Information Security Policy
2.2.3	ISO/IEC 2005:27002	06.1.8 Independent review of information security
2.2.9	ISO/IEC 2005:27002	08.2.2 Information security awareness, education, and training
3.2.1	ISO/IEC 2005:27002	06.1.2 Information security coordination
3.2.3 3.2.2	ISO/IEC 2005:27002	06.1.3: Define all IS responsibilities
3.2.4	ISO/IEC 2005:27002	06.1.4 Authorization process for information processing facilities
3.2.5	ISO/IEC 2005:27002	06.1.5 Confidentiality agreements
3.2.6 3.2.7	ISO/IEC 2005:27002	06.2.1 Identification of risks related to external parties
3.2.6 3.2.7	ISO/IEC 2005:27002	06.2.2 Addressing security when dealing with customers
3.2.6 3.2.7	ISO/IEC 2005:27002	06.2.3 Addressing security in third party agreements
3.2.7 4.2.6 Appendix D	ISO/IEC 2005:27002	10.02.1 Service delivery
3.2.7 4.2.6 Appendix D	ISO/IEC 2005:27002	10.02.2 Monitoring and review of third party services
3.2.7 4.2.6 6.2.2	ISO/IEC 2005:27002	10.02.3 Managing changes to third party services
4.2.1	ISO/IEC 2005:27002	08.1.2 Screening
4.2.2	ISO/IEC 2005:27002	08.1.3 Terms and conditions of employment
4.2.3	ISO/IEC 2005:27002	08.2.3 Disciplinary process
4.2.4	ISO/IEC 2005:27002	08.3.1: Termination Responsibilities
4.2.4	ISO/IEC 2005:27002	08.3.2: Return of assets
4.2.4	ISO/IEC 2005:27002	08.3.3: Removal of access rights
5.2.1	ISO/IEC 2005:27002	09.1.1 Physical security perimeter
5.2.10 5.2.11	ISO/IEC 2005:27002, NIST SP800-88, NISPOM2006-5220	09.2.6 Secure disposal or re-use of equipment
5.2.2	ISO/IEC 2005:27002	09.1.2 Physical entry controls
5.2.3	ISO/IEC 2005:27002	09.1.4: Protecting against external and environmental threats
5.2.3	ISO/IEC 2005:27002	09.2.1 Equipment citing and protection
5.2.4	ISO/IEC 2005:27002	09.1.3 Securing offices, rooms, and facilities
5.2.4	ISO/IEC 2005:27002	09.1.5 Working in secure areas
5.2.5	ISO/IEC 2005:27002	09.1.6: Public access, delivery/loading areas
5.2.6	ISO/IEC 2005:27002	09.2.2 Supporting utilities
5.2.7	ISO/IEC 2005:27002	09.2.3 Cabling Security

Policy Section	Source Title	Source Section
5.2.8	ISO/IEC 2005:27002	09.2.4 Equipment maintenance
5.2.9	ISO/IEC 2005:27002	09.2.5 Security of equipment off-premises
5.2.9	ISO/IEC 2005:27002	09.2.7 Removal of property
6.2.1	ISO/IEC 2005:27002	10.01.1 Documented operating procedures
6.2.10	ISO/IEC 2005:27002	10.10.5 Fault logging
6.2.11	ISO/IEC 2005:27002	10.06.1 Network controls
6.2.11	ISO/IEC 2005:27002	10.06.2 Security of network services
6.2.12	ISO/IEC 2005:27002	10.07.1 Management of removable media
6.2.12	ISO/IEC 2005:27002	10.07.2 Disposal of media
6.2.13	ISO/IEC 2005:27002	10.07.3 Information handling procedures
6.2.14	ISO/IEC 2005:27002	10.07.4 Security of system documentation
6.2.15	ISO/IEC 2005:27002	10.08.1 Information exchange policies and procedures
6.2.15	ISO/IEC 2005:27002	10.08.2 Exchange agreements
6.2.16	ISO/IEC 2005:27002	10.08.5 Business information systems
6.2.16	ISO/IEC 2005:27002	10.09.1 Electronic commerce
6.2.16	ISO/IEC 2005:27002	10.09.2 On-Line Transactions
6.2.17	ISO/IEC 2005:27002	10.08.4 Electronic messaging
6.2.17.2	ISO/IEC 2005:27002	15.1.4 Data protection and privacy of personal information
6.2.19	ISO/IEC 2005:27002	10.09.3 Publicly available information
6.2.2 - 6.2.2.4	ISO/IEC 2005:27002	10.01.2 Change management
6.2.20	ISO/IEC 2005:27002	10.10.6: Clock synchronization
6.2.21	ISO/IEC 2005:27002	12.6.1 Control of technical vulnerabilities
6.2.22	ISO/IEC 2005:27002	10.08.3 Physical media in transit
6.2.3	ISO/IEC 2005:27002	10.01.3: Segregation of duties
6.2.4	ISO/IEC 2005:27002	10.01.4 Separation of development, test, and operational facilities
6.2.5	ISO/IEC 2005:27002	10.03.1 Capacity management
6.2.6	ISO/IEC 2005:27002	10.03.2 System acceptance
6.2.7	ISO/IEC 2005:27002	10.04.1 Controls against malicious code
6.2.7	ISO/IEC 2005:27002	10.04.2: Control against mobile code
6.2.8	ISO/IEC 2005:27002	10.05.1 Information back-up
6.2.9	ISO/IEC 2005:27002	10.10.1 Audit logging
6.2.9	ISO/IEC 2005:27002	10.10.3 Protection of log information
6.2.9	ISO/IEC 2005:27002	10.10.4 Administrator and operator logs
7.2.1	ISO/IEC 2005:27002	11.1.1: Access Control Policy
7.2.1 7.2.3	ISO/IEC 2005:27002	11.4.1: Policy on use of network services
7.2.1.10	ISO/IEC 2005:27002	11.5.3 Password management system
7.2.1.2 7.2.3	ISO/IEC 2005:27002	11.4.2: User authentication for external connections
7.2.1.3	ISO/IEC 2005:27002	11.5.2 User identification and authentication

Policy Section	Source Title	Source Section
7.2.1.9 7.2.1.10 7.2.1.11	ISO/IEC 2005:27002	11.2.1: User registration 11.2.2: Privilege management 11.2.3: User password management 11.2.4: Review of user access rights
7.2.1.9 7.2.1.10 7.2.1.11	ISO/IEC 2005:27002	11.3.1 Password use
7.2.10	ISO/IEC 2005:27002	11.3.3 Clear desk and clear screen policy
7.2.2	ISO/IEC 2005:27002	11.3.2: Unattended user equipment
7.2.2	ISO/IEC 2005:27002	11.5.5 Session time-out
7.2.2	ISO/IEC 2005:27002	11.5.6 Limitation of connection time
7.2.3	ISO/IEC 2005:27002	11.4.3 Equipment identification in networks
7.2.3	ISO/IEC 2005:27002	11.4.4 Remote diagnostic and configuration port protection
7.2.3	ISO/IEC 2005:27002	11.4.5 Segregation in networks
7.2.3	ISO/IEC 2005:27002	11.4.6 Network connection control
7.2.3	ISO/IEC 2005:27002	11.4.7 Network routing control
7.2.5	ISO/IEC 2005:27002	11.5.4 Use of system utilities
7.2.5	ISO/IEC 2005:27002	11.6.1 Information access restriction
7.2.8	ISO/IEC 2005:27002	11.7.1 Mobile computing and communications
7.2.9	ISO/IEC 2005:27002	11.7.2 Teleworking
8.2.1 - 8.2.5 8.2.14 8.2.15	ISO/IEC 2005:27002	12.1.1: Security requirements analysis and specification 12.2.1: Input data validation 12.2.2: Control of internal processing 12.2.3: Message integrity 12.2.4: Output data validation 12.5.5: Outsourced software development 12.5.4 Information Leakage
8.2.10	ISO/IEC 2005:27002	12.5.1 Change control procedures
8.2.11	ISO/IEC 2005:27002	12.5.2 Technical review of applications after operating system changes
8.2.12	ISO/IEC 2005:27002	12.5.3 Restrictions on changes to software packages
8.2.6	ISO/IEC 2005:27002	12.3.1 Policy on the use of cryptographic controls
8.2.6	ISO/IEC 2005:27002	12.3.2 Key management
8.2.7	ISO/IEC 2005:27002	12.4.1 Control of operational software
8.2.8	ISO/IEC 2005:27002	12.4.2 Protection of system test data
8.2.9	ISO/IEC 2005:27002	12.4.3 Access control to program source code
8.2.1 - 8.2.5 8.2.14 8.2.15	ISO/IEC 2005:27002	12.1.1: Security requirements analysis and specification 12.2.1: Input data validation 12.2.2: Control of internal processing 12.2.3: Message integrity 12.2.4: Output data validation 12.5.5: Outsourced software development 12.5.4 Information Leakage
9.2.1	ISO/IEC 2005:27002	13.2.1 Responsibilities and procedures
9.2.1.1	ISO/IEC 2005:27002	13.1.1 Reporting information security events
9.2.2	ISO/IEC 2005:27002	13.2.2 Learning from information security incidents
9.2.3	ISO/IEC 2005:27002	13.2.3 Collection of evidence

Policy Section	Source Title	Source Section
9.2.6	ISO/IEC 2005:27002	13.1.2 Reporting security weaknesses
9.2.7	ISO/IEC 2005:27002	06.1.6 Contact with authorities
9.2.8	ISO/IEC 2005:27002	06.1.7 Contact with special interest groups
Appx D	ISO/IEC 2005:27002	08.1.1: Roles and responsibilities
Appx D	ISO/IEC 2005:27002	08.2.1 Management responsibilities
10.2.1-10.2.1.3	ISO/IEC 2005:27002	14.1.1 Including information security in the business continuity management process
10.2.1-10.2.1.3	ISO/IEC 2005:27002	14.1.2 Business continuity and risk assessment
10.2.1-10.2.1.3	ISO/IEC 2005:27002	14.1.3 Developing and implementing continuity plans including information security
10.2.1-10.2.1.3	ISO/IEC 2005:27002	14.1.4 Business continuity planning framework
10.2.1-10.2.1.3	ISO/IEC 2005:27002	14.1.5 Testing, maintaining and re-assessing business continuity plans
11.1.1	ISO/IEC 2005:27002	15.1.1 Identification of applicable legislation
11.1.2	ISO/IEC 2005:27002	15.1.2 Intellectual property rights (IPR)
11.2.4	ISO/IEC 2005:27002	15.2.1 Compliance with security policies and standards
11.2.5	ISO/IEC 2005:27002	15.2.2 Technical compliance checking
11.2.6	ISO/IEC 2005:27002	15.3.1: Information systems audit considerations 15.3.2: Protection of information systems audit tools
12.2	ISO/IEC 2005:27002	04.1: Risk Management
12.2	ISO/IEC 2005:27002	04.2: Treating Security Risks
12.2.1	NIST SP800-30	04.1: Risk Management, 04.2: Treating Security Risks

19 APPENDIX F: LEGISLATIVE POLICY DRIVERS

Title	Description
HIPAA (Health Insurance Portability and Accountability Act of 1996): HIPAA Security Rule (2003)	The Administrative Simplification provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA, Title II) required the Department of Health and Human Services (HHS) to establish national standards for the security of electronic health care information. The final rule adopting HIPAA standards for security was published in the Federal Register on February 20, 2003. This final rule specifies a series of administrative, technical, and physical security procedures for covered entities to use to assure the confidentiality of electronic protected health information. The standards are delineated into either required or addressable implementation specifications.
California State Civil Code §1798.81	Protection and Disposal of Personal Information
California State Civil Code §1798.82	Disclosure of Security Breech involving Personal Information
California State Civil Code §1798.83	Disclosure of Personal Information to Third-parties
California State Civil Code §1798.84	Explains violations of civil codes §1798.81 - 1798.84
California Senate Bill 1386 (2002)	Amended civil code §1798.82, §1798.84, and added California Notice of Security Breech Law (civil code §1798.29)
California Assembly Bill 1298 (2007)	Amended civil code §1798.29 & §1798.82, to include medical information as personal information

20 APPENDIX G: ACKNOWLEDGEMENT

By signing this document, I acknowledge that I have read, understand and will abide by the County of Orange Information Technology Security Policy.

Employee Name (please print): _____

Employee Signature: _____

Agency/Department: _____

Date: _____

INFORMATION TECHNOLOGY USAGE POLICY

COUNTY OF ORANGE

1 INTRODUCTION:

The County of Orange Information Technology (IT) Usage Policy is the foundation of the County's information security efforts. Each member of the County workforce is responsible for understanding his/her role in maintaining County IT security. This policy summarizes your information technology responsibilities. To learn more about information security, please see the Information Technology Security Policy.

Complete **Section 5: Acknowledgement** after you have finished reading this document. Your signature on the Acknowledgement indicates that you understand and will comply with County security policy. If you disregard security policies, standards, or procedures, you can be subject to County and agency-specific disciplinary action.

2 TERMS YOU NEED TO KNOW:

Authentication	The process of verifying the identity of anyone who wants to use County information before granting them access.
Back Up	To copy files to a second medium (for example, a disk or tape) as a precaution in case the first medium fails.
Confidentiality / Non-Disclosure Agreement	An agreement that outlines sensitive materials or knowledge that two or more parties wish to share with one another. By way of such agreement, the parties to the agreement agree not to share or discuss with outside parties the information covered by the agreement.
System or Software Configuration Files	Highly important files that control the operation of entire systems or software.
Electronic Communication	Messages sent and received electronically through any electronic text or voice transfer/storage system. This includes e-mail, text messages, instant messages (IM) and voicemail.
Encryption	The translation of data into a secret code. Encryption is the most effective way to achieve data security. To read an encrypted file, you must have access to a secret key or password that enables you to *decrypt* it. Unencrypted data is called *plain text*; encrypted data is referred to as *cipher text*.
Information Security	Safeguarding an organization's data from unauthorized access or modification to ensure its availability, confidentiality, and integrity.
Information Technology (IT)	The broad subject concerned with all aspects of managing and processing information within an organization.
Local Security Administrator (LSA)	The person at each agency who is responsible for the operational maintenance of IT security resources within the agency.
Network	Two or more linked computer systems. There are many different types of computer networks.
Password	Sequence of characters (letters, numbers, symbols) used in combination with a User ID to access a computer system or network. Passwords are used to authenticate the user before s/he gains access to the system.

Personally Identifiable Information (PII)	Any piece of information that could be used to uniquely identify, contact, or locate a single person. Examples include: full name; national identification number; email address; IP address; driver's license number; and Social Security Number.
User	Any individual who uses a computer.
User ID	Unique name given to a user for identification to a computer or telephone network, database, application, etc. Coupled with a password, it provides a minimal level of security.
Virus / Malicious Software	A software program that interferes with computer operation, damages or destroys electronic data, or spreads itself to other computers. Viruses and malicious software are often transmitted via email, documents attached to email, and the Internet.
Workforce Member	Any member of the County workforce, including employees, temporary help, contractors, vendors and volunteers.

3 POLICY OVERVIEW

As a member of the County workforce, you are expected to comply with the County's Information Technology Usage Policy. Your agency may have additional policies that you must follow as part of your job.

The following are key concepts of the County's policy:

- Information created or used in support of County business activities is the property of the County.
- Your assigned information technology resources are meant to facilitate the efficient and effective performance of your duties. It is your responsibility to ensure that resources are not misused and that you comply with policy.
- If you need to access confidential information as part of your duties, you will be asked to sign a confidentiality or non-disclosure agreement before you access the County network.
- Many County facilities house sensitive or critical information systems. You are expected to comply with all physical access controls designed to restrict unauthorized access.
- You may not remove County equipment or data in any format from the workplace unless you have received prior written approval from your supervisor or manager.
- The use of the network and Internet is a privilege, not a right. If you violate policy, you may lose your network and/or Internet access. The County may refuse to reinstate your access for the remainder of your employment at the County. The County may also take other disciplinary action as appropriate under County policy, departmental policy and applicable employment MOUs.

4 YOUR RESPONSIBILITIES

Your security responsibilities fall under several different Information Technology categories. Each category and the key responsibilities associated with it are listed below:

USER IDs AND PASSWORDS

- You will be issued a network user ID unique to you. Only you may use your user ID to access County resources (e.g. computer, telephone, FAX).
- You will be issued a default password at the same time as your user ID. You will be prompted to change your password the first time you log in to the system.
- Do not share user IDs and passwords with other users or individuals, including coworkers and supervisors. Treat your password as sensitive and highly confidential information.
- You are agreeing to follow the Information Technology Usage Policy when you accept a password from the County and use it to access the County data or telephone networks, the Internet, or the Intranet.
- Change your password immediately if you think someone else knows it. Report your suspicions to management.
- If you lose or forget your password, you are required to request a password reset. No one else can do it for you.

HARDWARE AND SOFTWARE

- The County will provide, and employees may request, peripheral equipment such as ear buds for cellular phones or Blackberry devices, as may be necessary to enable compliance with all local laws which pertain to the use of mobile communication equipment or the individual workplace needs for the employee to perform his or her employment.
- Never download or install any hardware or software without prior written approval of your agency IT representative.
- Do not make any changes to system and/or software configuration files unless specifically authorized in writing by your agency IT.
- Maintain your business data files on a network (or "shared") drive so that they can be backed up according to your agency's regular backup schedule.
- Use the "lock workstation" feature any time you leave your workstation logged on to the network and you are away from your desk.
- Do not connect a County laptop or other mobile device to the network until it has been scanned for viruses and malicious software.
- Follow the authentication procedures defined by your agency whenever you log in to the County network via Remote Access.
- Do not attempt to connect your workstation, laptop, or other computing device to the Internet via an unauthorized wireless or other connection while simultaneously connected to any County network.
- Retain original software installed on your computer if it is provided to you. The software must be available when your system is serviced in case it needs to be reinstalled.
- Do not keep liquids or magnets on or near computers, as they can cause serious damage.
- Ensure that your equipment is plugged into a surge protector at all times.

- Report all computer problems in detail on the appropriate form and/or when you contact the County Service Desk or discuss the problem with your agency's Help Desk.
- Report equipment damage immediately to the County Service Desk or your agency's Help Desk.

EMAIL and TELEPHONE

- The e-mail and telephone systems and networks are primarily for official County business.
- Management can freely inspect or review electronic mail and data files including voicemail. Employees should have no expectation of privacy regarding their internet usage, electronic mail or any other use of County computing or telephone equipment.
- Do not use a County email account or voicemail box assigned to another individual to send or receive messages unless you have been authorized, in writing, to act as that individual's delegate.
- Use of personal Internet (external) email systems from County networks and/or desktop devices is prohibited unless there is a compelling business reason for such use and prior written approval has been given by agency management and agency IT.
- Do not configure or use automated forwarding to send County email to Internet-based (external) email systems unless specifically authorized to do so, in writing, by County management.
- Send confidential information via email only with the written permission of management and only via an approved method. Mark the email according to agency policy.
- Treat confidential or restricted files sent as attachments to email messages as confidential or restricted documents. This also applies to confidential or restricted information embedded within an email message as message text or a voicemail message.
- Do not delete email or voicemail messages or other data if management has identified the subject matter as relevant to pending or anticipated litigation, personnel investigation, or other legal processes.

THE INTERNET / INTRANET

- Internet/Intranet access is primarily for County business.
- You may access the Internet for limited personal use only during nonworking time and in strict compliance with policy. If there is any doubt about whether an activity is appropriate, consult with your Department Head or his/her designee.

INFORMATION SECURITY

- Treat hardcopy or electronic Personally Identifiable Information (PII) as confidential and take all precautions necessary to ensure that it is not compromised. Intentional – or even accidental – disclosure of PII to unauthorized users is a violation of policy.
- Don't leave PII unattended or unsecured for any period of time.
- Be sure to follow your agency's policy for disposing of confidential data. This may include the physical destruction of data through shredding or other methods.
- Information created, sent, stored or received via the email system, network, Internet, telephones (including voicemail), fax or the Intranet is the property of the County.

- Do not expect information you create and store on County systems, including email messages or electronic files, to be private. Encrypting or using other measures to protect or "lock" an email message or an electronic file does not mean that the data are private.
- The County reserves the right to, at any time and without notice, access, read and review, monitor, and copy all messages and files on its computer system as it deems necessary.
- The County may disclose text or images to law enforcement without your consent as necessary.

PROHIBITED ACTIVITY

Unless you are specifically authorized by your manager or agency in writing, the following uses are prohibited by the Information Technology Security Policy:

- Using, transmitting, or seeking inappropriate or offensive materials, including but not limited to vulgar, profane, obscene, abusive, harassing, belligerent, threatening, or defamatory (harming another's reputation by lies) language or materials.
- Accessing, attempting to access, or encouraging others to access controversial or offensive materials.
- Revealing PII without permission, such as another's home address, telephone number, credit card number or Social Security Number.
- Making offensive or harassing statements or jokes about language, race, color, religion, national origin, veteran status, ancestry, disability, age, sex, or sexual orientation.
- Sending or soliciting sexually oriented messages, images, video or sound files.
- Visiting sites featuring pornography, terrorism, espionage, theft, drugs or other subjects that violate or encourage violation of the law.
- Gambling or engaging in any other activity in violation of local, state, or federal law.
- Uses or activities that violate the law or County policy or encourage others to violate the law or County policy. These include:
  - Accessing, transmitting, or seeking confidential information about clients or coworkers without proper authorization.
  - Intruding, or trying to intrude, into the folders, files, work, networks, or computers of others, or intercepting communications intended for others.
  - Knowingly downloading or transmitting confidential information without proper authorization.
- Uses that cause harm to others or damage to their property, including but not limited to:
  - Downloading or transmitting copyrighted materials without the permission of the copyright owner. Even if materials on the network or the Internet are not marked with the copyright symbol, ©, assume that they are protected under copyright law.
  - Using someone else's password to access the network or the Internet.
  - Impersonating another user or misleading message recipients into believing that someone other than the authenticated user is communicating a message.

- Uploading a virus, other harmful component, or corrupted data or vandalizing any part of the network.
- Creating, executing, forwarding, or introducing computer code designed to self-replicate, damage, or impede the performance of any computer's memory, storage, operating system, application software, or any other functionality.
- Engaging in activities that jeopardize the security of and access to the County network or other networks on the Internet.

- Downloading or using any software on the network other than that licensed or approved by the County.
- Conducting unauthorized business or commercial activities including, but not limited to:
  - Buying or selling anything over the Internet.
  - Soliciting or advertising the sale of any goods or services.
  - Unauthorized outside fund-raising activities, participation in any lobbying activity, or engaging in any prohibited partisan political activity.
  - Posting County, department and/or other public agency information to external news agencies, service bureaus, social networking sites, message boards, blogs or other forums.
- Uses that waste resources, including, but not limited to:
  - Printing of personal files.
  - Sending chain letters for any reason.
  - Including unnecessary recipients on an email. Only copy others on an email or voicemail message who should be "in the loop" on the topic addressed.
  - Indiscriminate use of distribution lists. Before using a distribution list, determine whether or not it is appropriate for everyone on that list to receive the email.
  - "All hands" emails. Emails of this type are to be sent only after management permission has been obtained.

5 ACKNOWLEDGEMENT

- If you violate security policies, standards, or procedures, you can be subject to County and agency-specific disciplinary action up to and including discharge.

By signing this document, I acknowledge that I have read, understand and will comply with this County of Orange Information Technology Usage Policy. I understand that the complete Information Technology Usage Policy is available for me to review on the County's intranet. I also may request a copy from the County Service Desk, my agency's Help Desk, or my agency's Local Security Administrator.

Workforce Member Name (please print): _____

Workforce Member Signature: _____

Agency/Department: _____

Date: _____

SOCIAL SERVICES AGENCY (SSA)
INFORMATION TECHNOLOGY SECURITY AND USAGE AGREEMENT

Declaration

I have read and agree to all provisions in the County of Orange Information Technology Security Policy, the County of Orange Information Technology Usage Policy, and the SSA Administrative Policies and Procedures Manual I 6 Information Technology Security and Usage. I will adhere to all applicable SSA, County of Orange, State of California, and Federal regulations relating to information technology security, privacy and confidentiality of information. I accept these responsibilities and agree to exercise proper care and to protect all assets while performing my duties. I understand that improper use of County resources and the disclosure of any sensitive, confidential, proprietary or Personal Identity Information (PII) to unauthorized persons during or after separation of my employment at SSA may make me liable for revocation of user privileges, discharge, and administrative, civil and/or criminal prosecution.

My signature below affirms I have read, understand and agree to the foregoing statements.

Print Name of User	Signature of User	Date

Supervisor of User/Human Resources (HR) Representative:

Print Name of Supervisor or HR Representative	Signature of Supervisor or HR Representative	Date

ORANGE COUNTY SOCIAL SERVICES AGENCY
CONFIDENTIALITY OF CLIENT INFORMATION

This policy has been established for the protection of clients of the Social Services Agency.

INSTRUCTIONS

1. Read the following policy statement carefully.

2. After you have read the policy statement, sign your name, and enter your social security number and date in the space provided. *The* signed statement will be placed in your personnel file.

POLICY CONCERNING THE CONFIDENTIALITY OF CLIENT INFORMATION

All written and oral information concerning clients of the Social Services Agency is confidential. The term clients, for purposes of this policy, shall include former, current, and future applicants, recipients, and authorized representatives who have received, are currently receiving, are currently seeking, or in the future will receive services from the Social Services Agency, including Children's Services, Adult and Employment Services, and Financial Assistance. It also includes all individuals who have been, who currently are, or who are pending potential future investigation in connection with the administration of Social Services Agency programs.

Information pertaining to clients of the agency shall not be disclosed to anyone, in or out of the workplace, including other employees, nor shall it be published, or used by any employee, except for purposes directly connected with the administration of agency programs as set forth in the California Welfare and Institutions Code, or pursuant to an order of a judge of the Juvenile Court.

This policy includes the names of persons, and all other personal or case-related information, including, but not limited to, client or case information in client case files; court reports; Juvenile Court records; internal agency memoranda, employee or agency reports, minutes and other documents; internal agency electronic mail and electronic messages; information contained in agency electronic data processing databases and systems; client or employee notes, documents, or correspondence; drafts of documents; and oral comments. If you are unsure if specific information is covered by this policy you must check with your supervisor before releasing this information.

I have read the above and acknowledge my responsibility to conform with this policy.

Signature _____ Date _____

SSN _____

°.F063.01-46 (11/96)

County of Orange Social Services Agency (SSA)

Administrative Policies and Procedures Manual

Number I 6

Placeholder for Attachment E

Social Services Agency Information Security Rules of the Road

Attachment E is an electronically based training to be completed by all SSA workforce members, contracted employees, volunteers, interns and contractor's personnel using County Equipment, etc.

Agreement to Comply with the Orange County Social Services Agency Administrative Policies and Procedures Manual I 6 Information Technology Security and Usage

I acknowledge that I have read, understand, and agree to abide by all provisions of the Orange County Social Services Agency (SSA) Administrative Policies and Procedures Manual I-6 Information Technology Security and Usage which can be found on the SSA Intranet in the Information Technology section.

SSA Information Security Rules of the Road

I also acknowledge that I have read and understand the Orange County SSA Information Security Rules of the Road which can be found on the SSA Intranet in the Training section.

Confidentiality Statement

I also agree to the terms stipulated in the Orange County SSA Confidentiality of Client Information which is provided below:

All written and oral information concerning clients of the Social Services Agency is confidential. The term clients, for purposes of this policy, shall include former, current, and future applicants, recipients, and authorized representatives who have received, are currently receiving, are currently seeking, or in the future will receive services from the Social Services Agency, including Children's Services, Adult and Employment Services, and Financial Assistance. It also includes all individuals who have been, who currently are, or who are pending potential future investigation in connection with the administration of Social Services Agency programs.

Information pertaining to clients of the agency shall not be disclosed to anyone, in or out of the workplace, including other employees, nor shall it be published, or used by any employee, except for purposes directly connected with the administration of agency programs as set forth in the California Welfare and Institutions Code, or pursuant to an order of a judge of the Juvenile Court.

This policy includes the names of persons, and all other personal or case-related information, including, but not limited to, client or case information in client case files; court reports; Juvenile Court records; internal agency memoranda, employee or agency reports, minutes and other documents; internal agency electronic mail and electronic messages; information contained in agency electronic data processing databases and systems; client or employee notes, documents, or correspondence; drafts of documents; and oral comments. If you are unsure if specific information is covered by this policy you must check with your supervisor before releasing this information.

SSA Workforce Member Printed Name_____

Signature _____ Date_____

Supervisor's Printed Name_____

Signature _____ Date_____

Retain this document for 3 years after the employee separates from SSA.

Loss of Personally Identifiable Information (PII) or Other Forms of Confidential Information

County of Orange Social Services Agency

Administrative Policies and Procedures Manual

Program/Area: Administration

Title: Loss of Personally Identifiable Information (PII) or Other Forms of Confidential Information

Number: I 7 **Status:** Updated

Effective Date: 2/28/17 **Revision Date:** 3/24/16

I. PURPOSE

To establish guidelines to expeditiously and accurately report lost Personally Identifiable Information and other forms of Confidential Information.

II. POLICY

All Social Services Agency (SSA/Agency) staff shall comply with all Federal and State requirements regarding the safeguarding of confidential information and reporting incident protocols. Compliance of this policy shall be in accordance with the State of California Department of Health Care Services (DHCS) Medi-Cal Privacy and Security Agreement (PSA) (Attachment A), the State of California Health and Human Services Agency Department of Social Services (CDSS) All County Letters No. 15-56 and 16-100 issued on August 14, 2015 (Attachment B) and January 12, 2016 (Attachment C) respectively, and the procedures outlined in Section IV below.

This policy applies to all data sources and systems with any PII and other forms of confidential information that staff access in the performance of their duties.

III. DEFINITIONS

Authorized Persons are employees of the Agency who meet the following criteria:

- Need to access PII and other forms of confidential information in order to perform their job duties;
- Have completed all required security and confidentiality training; and
- Have completed all required security certifications relevant to the data which are on file and available for review by an outside agency.

Confidential Information covers information that must be protected from unauthorized disclosure or public release. Examples of Confidential Information include but are not limited to the following: client case records, employment records, payroll and other financial information and other sensitive or business related information that is not intended for wide distribution.

Federal Tax Information (FTI) covers any data extracted from an individual's federal tax return (including attachments) that the Internal Revenue Service (IRS) provides to human services agencies under IRC §6103(l)(7). FTI is received from the following Income Earnings Verification System (IEVS) Reports:

- Annual IRS Asset Match (paper only) and
- Monthly Beneficiary Earnings Exchange Record (BEER) Match (paper only).

Lost PIIs or other forms of confidential information cover information containing PII or other forms of confidential information that a Deputy Director or delegated SSA manager has confirmed is no longer in the physical possession or control of an Agency representative; has been electronically transmitted to an unauthorized recipient; and/or has been accessed by an unauthorized user. This does not include information that has been misplaced within the confines of secured Agency facilities.

Personally Identifiable Information (PII) covers a combination of personal information stored electronically or in hard copy that describes the specific identity of the person such as a person's name with social security number (SSN) or date of birth (DOB). PII can be used to identify an individual person. For example, "Jane Doe" is not PII, but "Jane Doe DOB 1/1/1980" is PII.

Medi-Cal Personally Identifiable Information (Medi-Cal PII) covers information directly obtained in the course of performing an administrative function on behalf of Medi-Cal that can be used alone, or in conjunction with any other information to identify a specific individual. Medi-Cal PII includes any information that can be used to search for or identify individuals, or can be used to access their files, such as name, social security number, date of birth, driver's license number or identification number.

Security Breach is an unauthorized access or acquisition of information that compromises the security, confidentiality or integrity of PII. Information may be in electronic or hardcopy form and may consist of a single piece of information and/or an entire information system, such as hard drive, portable computer storage medium, Blackberry/Cell phones or laptop computer.

Examples of security breaches include but are not limited to:

- Faxing PII to a wrong number;
- A stolen electronic portable device containing PII;
- An employee's unauthorized access of data systems to inquire on an acquaintance;
- Improper disposal of records containing PII; and
- Leaving PII in a public place.

Social Security Administration Personally Identifiable Information covers PII received from the following Income Eligibility Verification System (IEVS) Reports:

- Monthly BEER Match (paper only);
- Payment Verification System (PVS) Match (electronic only);
- Integrated Earning Clearance/Fraud Detection System (IFD) Match (electronic only);
- Deceased Persons Match (DPM; paper only); and
- Nationwide Prisoner Match (NPM; paper or electronic).

SSA Staff refers to employees, contracted staff, volunteers, interns, trainees, and other persons whose work is under the direct control and oversight of SSA.

Unauthorized Access means audible or visual disclosure of PII without a direct business need or other lawful reason for use of this information.

IV. PROCEDURE

Specific reporting requirements related to a security breach are outlined below depending on the type of information:

(A) Loss of Medi-Cal PII as defined by the DHCS Medi-Cal PSA (Attachment A);

(B) Loss of Social Security Administration, Medi-Cal Eligibility Data System (MEDS) or Applicant Income and Eligibility Verification System (IEVS) PIIs as defined by the CDSS ACL 16-100 (Attachment C);

(C) Loss of Federal Tax Information (FTI) as defined by CDSS ACL 15-56 (Attachment B); or

(D) Loss of confidential information that does not meet (A), (B), or (C) (see Checklist, Attachment E and Attachment D, California SB 1386).

A. Reporting Process for Lost Medi-Cal PII

Within 24 hours (including weekends and holidays) of discovery of a security breach involving Medi-Cal PII, prompt reporting shall be undertaken following the steps below:

1. The SSA staff, upon discovery of lost Medi-Cal PII, shall report suspected loss through the chain-of-command up to the Deputy Director responsible for the affected unit.

2. The Deputy Director shall immediately direct the affected unit to attempt to locate the missing material(s) or information. If loss or unauthorized disclosure of Medi-Cal PII is confirmed, the Deputy Director or his/her

designee assumes the role of Action Officer who shall be responsible for handling all issues associated with this incident including communicating with stakeholders regarding current situation status, developing and implementing a remediation plan to mitigate damage and preventing further incidents from occurring.

3. The SSA staff knowledgeable about the incident shall submit a Special Incident Report (SIR) following Administrative Policies and Procedures F 13. The SIR should, at a minimum, include the same information as the DHCS notification message (see number 4 below).

4. The Action Officer shall also draft a DHCS Privacy Incident Report (PIR) using the information known about the incident at that time. The Action Officer shall use the most current version of this form, which is posted on the DHCS Privacy Office website (www.dhcs.ca.gov, select "Privacy & HIPAA" and then "County Use") or use this link: http://www.dhcs.ca.gov/formsandpubs/laws/priv/Pages/CountiesOnly.aspx.

5. The Agency Director or his/her designee shall review the DHCS notification message and, if necessary, direct the Action Officer to notify County Counsel, Risk Management and/or the County Executive Office of the incident.

6. If the incident meets any of the criteria noted in the County Significant Incident/ Claim Reporting Protocol, the Action Officer shall draft a report containing the basic/concise facts and recommend approval by their Deputy Director to promptly send it via mail to IncidentReport@ocgov.com.

7. Once approved by the Agency Director or his/her designee, the Action Officer shall ensure that DHCS is provided with the information on the notification message PIR by telephone call or e-mail within one working day of discovery. The PIR shall be sent to the DHCS Privacy Office and the DHCS Information Security Office with a copy to CDSS Information Security and Privacy Office. The DHCS is acting on behalf of CDSS, for purposes of receiving reports of privacy and information security incidents and breaches.

DHCS Privacy Office	DHCS Information Security Office
DHCS Privacy Office c/o: Office of HIPAA Compliance MS 4722 P.O. Box 997413 Sacramento, CA 95899-7413 Email: privacyofficer@dhcs.ca.gov Telephone: (916) 445-4646 or (866) 866-0602	DHCS Information Security Office MS 6400 P.O. Box 997413 Sacramento, CA 95899-7413 Email: iso@dhcs.ca.gov Telephone: EITS Service Desk (916) 440-7000 or (800) 579-0874
CDSS Information Security & Privacy Office California Department of Social Services Information Security & Privacy Office 744 P Street, MS 9-9-70 Sacramento, CA 95814-6413 Email: iso@dss.ca.gov Telephone: (916) 651-5558	

8. The Action Officer shall initiate and ensure that prompt corrective action is taken to mitigate any risks or damages involved with the breach, and to protect the operating environment.

9. The Action Officer shall oversee the completion of the breach investigation and submit reports to the DHCS Privacy Officer and Information Security Officer in accordance with PSA directions.

10. The Action Officer shall oversee notification of individuals affected by the breach or unauthorized use/disclosure of Medi-Cal PII when notification is required. The Action Officer shall contact County Counsel and Risk Management, and also obtain the approval of the DHCS Privacy Officer for the time, manner and content of any such required notifications.

B. Reporting Process for Lost Social Security Administration, MEDS or IEVS PIIs

(Note: Although Social Security Administration, MEDS, and IEVS PIIs are governed by CDSS, DHCS breach reporting procedures are used and CDSS is copied on reports).

Loss of Social Security Administration PII shall be reported within an hour of discovery. While discovery of a security breach involving MEDS or IEVS PII PII, shall be reported within 24 hours (including weekends and holidays). Reporting shall be undertaken following the steps below:

1. The SSA staff, upon discovery of lost Social Security Administration, MEDS, or IEVS PIIs, shall report suspected loss through the chain-of-command up to the Deputy Director responsible for the affected unit.

2. The Deputy Director shall immediately direct the affected unit to attempt to locate the missing material(s) or information. If loss or unauthorized disclosure of PII is confirmed, the Deputy Director or his/her designee assumes the role of Action Officer who shall be responsible for handling all issues associated with this incident including communicating with stakeholders regarding current situation status, developing and implementing a remediation plan to mitigate damage and preventing further incidents from occurring.

3. The SSA staff knowledgeable about the incident shall submit a Special Incident Report (SIR) following Administrative Policies and Procedures F 13. The SIR should, at a minimum, include the same information as the DHCS notification message (see number 4 below).

4. The Action Officer shall also draft a Privacy Incident Report (PIR) using the information known about the incident at that time. The Action Officer shall use the most current version of this form, which is posted on the DHCS (both DHCS and CDSS use the same form) Privacy Office website (www.dhcs.ca.gov, select "Privacy & HIPAA" and then "County Use") or use this link: http://www.dhcs.ca.gov/formsandpubs/laws/priv/Pages/CountiesOnly.aspx.

5. The Agency Director or his/her designee shall review the notification message and, if necessary, direct the Action Officer to notify County Counsel, Risk Management and/or the County Executive Office of the incident.

6. If the incident meets any of the criteria noted in the County Significant Incident/ Claim Reporting Protocol, the Action Officer shall draft a report containing the basic/concise facts and recommend approval by their Deputy Director to promptly send it via mail to IncidentReport@ocgov.com.

7. Once approved by the Agency Director or his/her designee, the Action Officer shall ensure that DHCS and CDSS is provided with the information on the notification message PIR by telephone call or e-mail within one working day of discovery. The PIR shall be sent to the DHCS Privacy Office and the DHCS Information Security Office with a copy to CDSS Information Security and Privacy Office. The DHCS is acting on behalf of CDSS, for purposes of receiving reports of privacy and information security incidents and breaches.

DHCS Privacy Office	DHCS Information Security Office
DHCS Privacy Office c/o: Office of HIPAA Compliance MS 4722 P.O. Box 997413 Sacramento, CA 95899-7413 Email: privacyofficer@dhcs.ca.gov Telephone: (916) 445-4646 or (866) 866-0602	DHCS Information Security Office MS 6400 P.O. Box 997413 Sacramento, CA 95899-7413 Email: iso@dhcs.ca.gov Telephone: EITS Service Desk (916) 440-7000 or (800) 579-0874
CDSS Information Security & Privacy Office California Department of Social Services Information Security & Privacy Office 744 P Street, MS 9-9-70 Sacramento, CA 95814-6413 Email: iso@dss.ca.gov Telephone: (916) 651-5558	

8. The Action Officer shall initiate and ensure that prompt corrective action is taken to mitigate any risks or damages involved with the breach, and to protect the operating environment.

9. The Action Officer shall oversee the completion of the breach investigation and submit reports to the DHCS Privacy Officer and Information Security Officer in accordance with PSA directions.

10. The Action Officer shall oversee notification of individuals affected by the breach or unauthorized use/disclosure of PII when notification is required. The Action Officer shall contact County Counsel and Risk Management, and also obtain the approval of the DHCS Privacy Officer for the time, manner and content of any such required notifications.

C. Reporting Process for Loss of FTI

A discovery of a security breach involving loss of FTI shall be reported within 24 hours (including weekends and holidays) of discovery. Follow the reporting guidelines stated in Section IV, A. 1 through 5 and 7; and reporting protocols to the appropriate parties, using the guidelines provided by the State of California Health and Human Services Agency Department of Social Services All County Letter No. 15-56 issued on August 14, 2015 (Attachment B). (Do not contact DHCS).

In addition, the following steps shall be immediately followed by the Action Officer:

1. Review SIR document and if necessary, notify County Counsel, Risk Management and/or the County Executive Office of the incident. If the incident meets any of the criteria noted in the County Significant Incident/Claim Reporting Protocol, the Action Officer shall advise the Division Director to send the basic/concise facts by email to IncidentReport@ocgov.com promptly.

2. Complete the breach investigation and submit a written breach report within five working days of the incident to the Agency Director detailing the following:

- The data elements which were involved;
- A description of the unauthorized persons known or reasonably believed to have improperly used or disclosed confidential information;
- A list of the names of those people whose confidential information was disclosed;
- County Counsel recommendation on how, when and the content of the notification to those people whose confidential information was disclosed;
- A description of where the confidential information is believed to have been improperly transmitted, sent, or used;
- A description of the probable causes of the breach; and
- A detailed corrective action plan including measures that were taken to halt and/or contain the breach and recommendations on how to prevent future breaches.

3. If required, oversee notification of individuals affected by the security breach upon approval of the Agency Director or his/her designee;

Note: If security breach was reported to IRS Office of Safeguards, the Agency Director/designee shall inform the IRS office of notification activities undertaken before the notifications are released to the impacted individuals. In addition, the Agency/designee shall inform the IRS Office of Safeguards of any pending media release, including sharing the text, prior to distribution.

4. Ensure implementation of the corrective action plan and periodically report progress to the Agency Director.

D. Reporting Process for Loss or Unauthorized Disclosure of Confidential Information except Medi-Cal, Social Security Administration, MEDS, IEVS, or FTI PIIs.

SSA staff and Deputy Directors shall follow any applicable guidelines stated in Section IV A, B, or Attachment C.

California Civil Code 1798.29 requires notifying California residents whose unencrypted personal information was, or is reasonably believed to have been acquired by an unauthorized person of the data breach discovery.

In case of loss or unauthorized disclosure of PII, the Agency must notify in writing those people whose personal information was lost or disclosed.

EXCEPTION: There is no requirement to notify individuals if the personal information was encrypted.

E. Reporting process outlined in the Children and Family Services Division (CFS Policy F-0105), Loss/Theft of Client Personal Information shall also be followed by CFS staff as appropriate, in addition to the above procedure.

V. REFERENCES

California Department of Social Services, Privacy and Security Agreement, ACL 16-100 dated January 12, 2017

California SB 1386 Personal Information: Privacy

California Civil Code 1798.29

Children and Family Services Division (CFS Policy F-0105), Loss/Theft of Client Personal Information

County Executive Office Memorandum from Mark Denny, Chief Operating Officer, Subject: Significant Incident/Claim Reporting Protocol dated November 5, 2013

Department of Health Care Services 2016 Medi-Cal Privacy and Security Agreements, ACWDL 16-09 dated May 3, 2016

VI. ATTACHMENTS

A. Medi-Cal Privacy and Security Agreement between the California Department of Health Care Services and the County of Orange, Social Services Agency

B. California Department of Social Services All County Letter No. 15-56 titled Information Security Incident Reporting Protocol for Federal Tax Information and Personally Identifying Information, August 14, 2015

C. California Department of Social Services, Privacy and Security Agreement ACL 16-100 dated January 12, 2017

D. California SB 1386 Personal Information: Privacy

E. Checklist: Reporting Protocols

RHEIS Data Use And Disclosure Agreement

This California Refugee Health Electronic Information System (**RHEIS**) Data Use And Disclosure Agreement (hereinafter referred to as "Agreement") sets forth the information privacy and security requirements that the _____ **Department of Public Health** (hereinafter "Data Recipient") is obligated to follow with respect to all RHEIS System Data, and other personal and confidential information, (as each of these types of data and information are defined herein), disclosed to Data Recipient by the California Department of Public Health (hereinafter "CDPH"). (Such RHEIS System Data and other personal and confidential information are also referred to herein collectively as "Protected Data.") This Agreement covers Protected Data in any medium (paper, electronic, oral) in which the Protected Data exists. By entering into this Agreement, CDPH and Data Recipient desire to protect the privacy and provide for the security of all Protected Data in compliance with all state and federal laws applicable to the Protected Data. Permission to receive, use and disclose Protected Data requires execution of this Agreement that describes the terms, conditions and limitations of Data Recipient's collection, use and disclosure of the Protected Data.

I. Supersession: This Agreement supersedes Agreement Number None, dated None, between CDPH and Data Recipient.

II. Definitions: For purposes of this Agreement, the following definitions shall apply:

A. Breach: "Breach" means:

1. the acquisition, access, use, or disclosure of Protected Data, in any medium (paper, electronic, oral), in violation of any state or federal law or in a manner not permitted under this Agreement, that compromises the privacy, security or integrity of the information. For purposes of this definition, "compromises the privacy, security or integrity of the information" means poses a significant risk of financial, reputational, or other harm to an individual or individuals; or

2. the same as the definition of "breach of the security of the system" set forth in California Civil Code section 1798.29, subdivision (f).

B. Confidential Information: "Confidential Information" means information that:

1. does not meet the definition of "public records" set forth in California Government Code section 6252, subdivision (e), or is exempt from disclosure under any of the provisions of Section 6250, et seq. of the California Government Code or any other applicable state or federal laws; or

2. is contained in documents, files, folders, books, or records that are clearly labeled, marked, or designated with the word "confidential" by CDPH; or

3. is "personal information" as defined in this Agreement; or

4. meets the definition of "confidential public health record or records" as set forth in California Health and Safety Code section 121035, subdivision (c) if the record or records contains or consists of information relating to human immunodeficiency virus (HIV) or acquired immunodeficiency syndrome (AIDS).

C. Disclosure: "Disclosure" means the release, transfer, provision of, access to, or divulging in any other manner of information. "Disclosure" includes the disclosure, release, transfer, dissemination, or communication of all or any part of any confidential research record orally, in writing, or by electronic means to any person or entity, or providing the means for obtaining the records.

D. Refugee Health Electronic Information Exchange (RHEIS) System Data: "Refugee Health Electronic Information Exchange (RHEIS) System Data" means data in or from the RHEIS database owned and maintained by CDPH of refugee demographic, clinical, and administrative information. RHEIS data specifically includes information contained in, extracted or derived from the following:

1. California Refugee Health Assessment Form (CDPH 8418A); and

2. Administrative data collected in RHEIS.

E. Personal Information: "Personal Information" means information that:

1. by itself directly identifies or uniquely describes an individual; or

2. creates a substantial risk that it could be used in combination with other information to indirectly identify or uniquely describe an individual, or link an individual to the other information; or

3. meets the definition of "personal information" set forth in California Civil Code section 1798.3, subdivision (a); or

4. is one of the data elements set forth in California Civil Code section 1798.29, subdivisions (g)(1) and/or (2); or

5. meets the definition of "medical information" set forth in either California Civil Code section 1798.29, subdivision (h)(2) or California Civil Code section 56.05, subdivision (j); or

6. meets the definition of "health insurance information" set forth in California Civil Code section 1798.29, subdivision (h)(3).

F. Protected Data: "Protected Data" means data that consists of one or more of the following types of information :

1. "Refugee Health Information Exchange (RHEIS) System Data," as defined above; or

2. "Personal Information," as defined above; or

3. "Confidential Information," as defined above.

G. Security Incident: "Security Incident" means:

1. an attempted breach; or

2. the attempted or successful modification or destruction of Protected Data, in violation of any state or federal law or in a manner not permitted under this Agreement; or

3. the attempted or successful modification or destruction of, or interference with, Data Recipient's system operations in an information technology system, that negatively impacts the confidentiality, availability or integrity of Protected Data, or hinders or makes impossible Data Recipient's receipt, collection, creation, storage, transmission or use of Protected Data by Data Recipient pursuant to this Agreement.

H. Use: "Use" means the sharing, employment, application, utilization, examination, or analysis of information.

III. Background and Purpose: The CDPH, Office of Refugee Health (ORH) provides federal funding to impacted local health jurisdictions (LHJs) to provide post-arrival health assessments to all new refugees coming to California. LHJs are also required to enter health assessment results into RHEIS. RHEIS is a secure web-based application that the ORH has implemented for surveillance of communicable diseases, monitoring of chronic and mental health conditions, and to evaluate performance of contracted LHJs. LHJs and CDPH have access to data reports, in real-time, as needed, for referring patients to primary health and mental health services providers and to evaluate overall program performance. RHEIS is an integral part of the overall California Refugee Health Program's mission to assist refugees to get healthy and stay healthy so that they can achieve self-sufficiency.

IV. Legal Authority for Use and Disclosure of Protected Data: The legal authority for CDPH to collect, use and disclose Protected Data, and for Data Recipient to receive and use Protected Data is set forth in Attachment A.

V. Permitted Use and Disclosure of Protected Data:

A. The Data Recipient and its employees or agents, shall not use any Protected Data for any purpose other than carrying out the Data Recipient's obligations under the statutes and regulations set forth in Section IV above, or as identified

for the following purposes, set forth in this Section, below, or as otherwise allowed or required by state or federal law.

1. Assist LHJs with client transportation and interpretation services to ensure that timely and effective continuum of care for refugees is provided.

2. Provide each refugee case with a general orientation to the health care system in the resettlement area, including health assessment services available through state or local public or private health programs;

3. Assist refugees in obtaining a health screening within thirty days of arrival;

4. Encourage and assist refugees as soon as possible after arrival to obtain immunizations and, as required for adjustment to permanent resident alien status one year after arrival;

5. Assist refugees in accessing appropriate providers of continued therapy or preventive treatment for health conditions affecting public health; and

6. In the case of a refugee who fails or refuses to receive health screenings, provide additional information and counseling to the refugee, including an explanation of local health regulations and practices, and document the circumstances and action taken in the case file.

B. CDPH will provide a unique username and password for each individual accessing the RHEIS secured database, on behalf of Data Recipient. If there are personnel changes to the Data Recipient's user account designees, Data Recipient shall immediately notify the CDPH RHEIS contact identified in Section XIII(E), below, upon which time that user account shall be cancelled.

VI. Safeguards: Data Recipient shall implement administrative, physical, and technical safeguards that reasonably and appropriately protect the privacy, confidentiality, security, integrity, and availability of Protected Data, including electronic or computerized Protected Data. The Data Recipient shall develop and maintain a written information privacy and security program that includes administrative, technical and physical safeguards appropriate to the size and complexity of the Data Recipient's operations and the nature and scope of its activities in performing its legal obligations and duties (including performance of its duties and obligations under this Agreement), and which incorporates the requirements of Section VIII, Security, below. Data Recipient shall provide CDPH with Data Recipient's current and updated policies.

VII. California HIV/AIDS-Specific Statutes Pertaining to Confidential Public Health Records and Penalties for Disclosures: Any HIV/AIDS related information collected or maintained by CDPH (or its agents or contractors) or a local health department or agency (or its agent or

contractors), that may directly or indirectly identify an individual are considered confidential public health record(s) under California Health and Safety Code (HSC) Section 121035(c) and must be handled with the utmost confidentiality. Furthermore, HSC Section 121025(a) prohibits the disclosure of HIV/AIDS-related public health records that contain any personally identifying information to any third-party, unless authorized by law for public health purposes, or by the written consent of the individual identified in the record or his/her guardian/conservator. Except as permitted by law, any person who negligently discloses information contained in a confidential public health record to a third party is subject to a civil penalty of up to $5,000 plus court costs, as provided in HSC Section 121025(e)(1). Any person who willfully or maliciously discloses the content of a public health record, except as authorized by law, is subject to a civil penalty of $5,000-$25,000 plus court costs as provided by HSC Section 121025(e)(2). Any willful, malicious, or negligent disclosure of information contained in a public health record in violation of state law that results in economic, bodily, psychological harm to a person named in the record is a misdemeanor, punishable by imprisonment for a period of up to one year and/or a fine of up to $25,000 plus court costs. [HSC Section 121025(e)(3).] Any person who is guilty of a confidentiality violation of the foregoing type may be sued by the injured party and shall be personally liable for all actual damages incurred for economic, bodily, or psychological harm as a result of the breach. [HSC Section 121025(e)(4).] Each disclosure in violation of California law is a separate, actionable offense. [HSC Section 121025(e)(5).]

VIII. Security: The Data Recipient shall take all steps necessary to ensure the continuous security of all computerized data systems containing Protected Data. These steps shall include, at a minimum:

A. complying with all applicable CDPH data system security statutory and regulatory, compliance requirements, see http://cdphintranet/technology/ISO/Documents/CDPH%20Info%20Sec%20Policy%20-%20Aug%202010.pdf, and the data system security precautions listed in the Data Recipient Data Security Standards set forth in Attachment B to this Agreement;

B. providing a level and scope of security that is at least comparable to the level and scope of security established by the Office of Management and Budget in OMB Circular No. A-130, Appendix III - Security of Federal Automated Information Systems, which sets forth guidelines for automated information systems in federal agencies; and

C. in case of a conflict between any of the security standards contained in any of the aforementioned sources of security standards, the most stringent shall apply. The most stringent means that safeguard which provides the highest level of protection to Protected Data from breaches and security incidents.

IX. Security Officer: The Data Recipient shall designate a Security Officer to oversee its compliance with this Agreement and for communicating with CDPH on matters concerning this Agreement.

X. Training: The Data Recipient shall provide training on its obligations under this Agreement, at its own expense, to all of its employees and workforce who assist in the performance of Data Recipient's obligations under this Agreement, or otherwise use or disclose Protected Data.

A. The Data Recipient shall require each employee who receives training attain a certification, indicating the employee's name and the date on which the training was completed.

B. The Data Recipient shall retain each employee's written certifications of trainings for CDPH inspection for a period of three years following contract termination.

XI. Employee Discipline: Data Recipient shall discipline such employees and other Data Recipient workforce members who intentionally violate any provisions of this Agreement, including, if warranted, by termination of employment.

XII. Employee/Data Recipient Security and Confidentiality Agreement: Prior to accessing Protected Data, Data Recipient employees and Data Recipients will sign CDPH's confidentiality agreement, provide signed copies of these agreements to CDPH and review these agreements annually as required by law (see Attachment C, "Agreement by Employee/Data Recipient to Comply with Confidentiality Requirements" (CDPH 8689)).

XIII. Breach and Security Incident Responsibilities:

A. Notification to CDPH of Breach or Security Incident: The Data Recipient shall notify CDPH **immediately by telephone call plus email or fax** upon the discovery of a breach (as defined in this Agreement), **or** within **twenty-four (24) hours by email or fax** of the discovery of any security incident (as defined in this Agreement). Notification shall be provided to the CDPH Program Manager, the CDPH Privacy Officer and the CDPH Chief Information Security Officer, using the contact information listed in Section XIII(E), below. If the breach or security incident occurs after business hours or on a weekend or holiday and involves Protected Data in electronic or computerized form, notification to CDPH shall be provided by calling the CDPH IT Service Desk at the telephone numbers listed in Section XIII(E), below. For purposes of this Section, breaches and security incidents shall be treated as discovered by Data Recipient as of the first day on which such breach or security incident is known to the Data Recipient, or, by exercising reasonable diligence would have been known to the Data Recipient. Data Recipient shall be deemed to have knowledge of a breach or security incident if such breach or security incident is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach or security incident, who is an employee or agent of the Data Recipient.
Data Recipient shall take:

1. prompt corrective action to mitigate any risks or damages involved with the breach or security incident and to protect the operating environment; and

2. any action pertaining to a breach required by applicable federal and state laws, including, specifically, California Civil Code section 1798.29.

B. Investigation of Breach: The Data Recipient shall immediately investigate such breach or security incident, and within seventy-two (72) hours of the discovery, shall inform the CDPH Help Desk, the CDPH Privacy Officer, and the CDPH Chief Information Security Officer of:

1. what data elements were involved and the extent of the data involved in the breach, including, specifically, the number of individuals whose personal information was breached; and

2. a description of the unauthorized persons known or reasonably believed to have improperly used, accessed or disclosed the Protected Data and/or a description of the unauthorized persons known or reasonably believed to have improperly accessed or acquired the Protected Data, or to whom it is known or reasonably believe have had the Protected Data improperly disclosed to them; and

3. a description of where the Protected Data is believed to have been improperly accessed, used or disclosed; and

4. a description of the probable causes of the breach or security incident; and

5. whether Civil Code Section 1798.29 or any other federal or state laws requiring individual notifications of breaches have been triggered.

C. Written Report: The Data Recipient shall provide a written report of the investigation to the CDPH Program Manager, the CDPH Privacy Officer, and the CDPH Chief Information Security Officer within five (5) working days of the discovery of the breach or security incident. The report shall include, but not be limited to, the information specified above, as well as a full, detailed corrective action plan, including information on measures that were taken to halt and/or contain the breach or security incident, and measures to be taken to prevent the recurrence of such breach or security incident.

D. Notification to Individuals: If notification to individuals whose information was breached is required under state or federal law, and regardless of whether Data Recipient is considered only a custodian and/or non-owner of the Protected Data, Data Recipient shall, at its sole expense, and at the sole election of CDPH, either:

1. make notification to the individuals affected by the breach (including substitute notification), pursuant to the content and timeliness provisions of such applicable state or federal breach notice laws. The CDPH Privacy Officer shall approve the time, manner and content of any such notifications, prior to the transmission of such notifications to the individuals; or

2. cooperate with and assist CDPH in its notification (including substitute notification) to the individuals affected by the breach.

E. CDPH Contact Information: To direct communications to the above referenced CDPH staff, the Data Recipient shall initiate contact as indicated herein. CDPH reserves the right to make changes to the contact information below by giving written notice to the Data Recipient. Said changes shall not require an amendment to this Agreement.

CDPH Program Manager	CDPH Privacy Officer	CDPH Chief Information Security Officer (and CDPH IT Service Desk)
Office of Refugee Health P.O. Box Sacramento, CA 95899-7377 California Department of Public Health Email: Marisa.Ramos@cdph.ca.gov Telephone: (916) 552-8252	**Privacy Officer** Privacy Office, c/o Office of Legal Services California Department of Public Health 1415 L Street, Suite 500 Sacramento, CA 95814 Email: privacy@cdph.ca.gov Telephone: (877) 421-9634	**Chief Information Security Officer** Information Security Office California Department of Public Health P.O. Box 997413, MS 6302 Sacramento, CA 95899-7413 Email: cdphiso@cdph.ca.gov Telephone: IT Service Desk (916) 440-7000 or (800) 579-0874

XIV. Indemnification: Data Recipient shall indemnify, hold harmless and defend CDPH from and against any and all claims, losses, liabilities, damages, costs and other expenses (including attorney fees) that result from or arise directly or indirectly out of or in connection with any negligent act or omission or willful misconduct of Data Recipient, its officers, employees or agents relative to the Protected Data, including without limitation, any violations of Data Recipient's responsibilities under this Agreement.

XV. Term of Agreement: This Agreement shall remain in effect for three (3) years after the latest signature date in the signature block below. After three (3) years, this Agreement will expire without further action. If the parties wish to extend this Agreement, they may do so by reviewing, updating, and reauthorizing this Agreement. The newly signed agreement should explicitly supersede this Agreement, which should be referenced by agreement number and date in Section I of the new agreement. If one or both of the parties wish to terminate this Agreement prematurely, they may do so upon 30 days advanced notice. CDPH may also terminate this Agreement pursuant to Sections XVI or XVIII, below.

XVI. Termination for Cause:

A. Termination Upon Breach: A breach by Data Recipient of any provision of this Agreement, as determined by CDPH, shall constitute a material breach of the Agreement and grounds for immediate termination of the Agreement by CDPH. At its sole discretion, CDPH may give Data Recipient 30 days to cure the breach.

B. Judicial or Administrative Proceedings: Data Recipient will notify CDPH if it is named as a defendant in a criminal proceeding related to a violation of this

Agreement. CDPH may terminate the Agreement if Data Recipient is found guilty of a criminal violation related to a violation of this Agreement. CDPH may terminate the Agreement if a finding or stipulation that the Data Recipient has violated any security or privacy laws is made in any administrative or civil proceeding in which the Data Recipient is a party or has been joined.

XVII. Return or Destruction of Protected Data upon Expiration or Termination: Upon expiration or termination of the agreement between Data Recipient and CDPH for any reason, Data Recipient shall return or destroy the Protected Data. If return or destruction is not feasible, Data Recipient shall explain to CDPH why, in writing, to the CDPH Help Desk, the CDPH Privacy Officer and the CDPH Chief Information Security Officer, using the contact information listed in Section XIII(E), above.

A. Retention Required by Law: If Required by state or federal law, Data Recipient may retain, after expiration or termination, Protected Data for the time specified as necessary to comply with the law.

B. Obligations Continue Until Return or Destruction: Data Recipient's obligations under this Agreement shall continue until Data Recipient destroys the Protected Data or returns the Protected Data to CDPH; provided however, that on expiration or termination of the Agreement, Data Recipient shall not further use or disclose the Protected Data except as required by state or federal law.

C. Notification of Election to Destroy Protected Data: If Data Recipient elects to destroy the Protected Data, Data Recipient shall certify in writing, to the CDPH Program Manager, the CDPH Privacy Officer and the CDPH Chief Information Security Officer, using the contact information listed in Section XIII(E), above, that the Protected Data has been destroyed.

XVIII. Amendment: The parties acknowledge that federal and state laws relating to information security and privacy are rapidly evolving and that amendment of this Agreement may be required to provide for procedures to ensure compliance with such laws. The parties specifically agree to take such action as is necessary to implement new standards and requirements imposed by regulations and other applicable laws relating to the security or privacy of Protected Data. Upon CDPH's request, Data Recipient agrees to promptly enter into negotiations with CDPH concerning an amendment to this Agreement embodying written assurances consistent with new standards and requirements imposed by regulations and other applicable laws. CDPH may terminate this Agreement upon thirty (30) days written notice in the event:

A. Data Recipient does not promptly enter into negotiations to amend this Agreement when requested by CDPH pursuant to this Section or

B. Data Recipient does not enter into an amendment providing assurances regarding the safeguarding of Protected Data that CDPH in its sole discretion deems sufficient to satisfy the standards and requirements of applicable laws and regulations relating to the security or privacy of Protected Data.

XIX. Assistance in Litigation or Administrative Proceedings: Data Recipient shall make itself and any employees or agents assisting Data Recipient in the performance of its obligations under this Agreement, available to CDPH at no cost to CDPH to testify as witnesses, or otherwise, in the event of litigation or administrative proceedings being commenced against CDPH, its director, officers or employees based upon claimed violation of laws relating to security and privacy, which involves inactions or actions by the Data Recipient, except where Data Recipient or its employee or agent is a named adverse party.

XX. Disclaimer: CDPH makes no warranty or representation that compliance by Data Recipient with this Agreement will be adequate or satisfactory for Data Recipient's own purposes or that any information in Data Recipient's possession or control, or transmitted or received by Data Recipient, is or will be secure from unauthorized use or disclosure. Data Recipient is solely responsible for all decisions made by Data Recipient regarding the safeguarding of Protected Data.

XXI. Transfer of Rights: Data Recipient has no right and shall not subcontract, delegate, assign, or otherwise transfer or delegate any of its rights or obligations under this Agreement to any other person or entity. Any such transfer of rights shall be null and void.

XXII. No Third-Party Beneficiaries: Nothing express or implied in the terms and conditions of this Agreement is intended to confer, nor shall anything herein confer, upon any person other than CDPH or Data Recipient and their respective successors or assignees, any rights, remedies, obligations or liabilities whatsoever.

XXIII. Interpretation: The terms and conditions in this Agreement shall be interpreted as broadly as necessary to implement and comply with regulations and applicable state and federal laws. The parties agree that any ambiguity in the terms and conditions of this Agreement shall be resolved in favor of a meaning that is consistent and complies with federal and state laws.

XXIV. Survival: The respective rights and obligations of Data Recipient under Sections VI, VIII, XIII and XVII of this Agreement shall survive the termination or expiration of this Agreement.

XXV. Entire Agreement: This Agreement constitutes the entire agreement between CDPH and Data Recipient. Any and all modifications of this Agreement must be in writing and signed by all parties. Any oral representations or agreements between the parties shall be of no force or effect.

XXVI. Severability: The invalidity in whole or in part of any provisions of this Agreement shall not void or affect the validity of any other provisions of this Agreement.

XXVII. Signatures:

IN WITNESS, WHEREOF, the Parties have executed this Agreement as follows:

On behalf of the **Data Recipient**, the undersigned individual hereby attests that he or she is authorized to enter into this Agreement and agrees to all the terms specified herein.

Name (Print)	Name (Sign)
Title (County Official)	Date

On behalf of the **Department of Public Health**, the undersigned individual(s) hereby attests that he or she is authorized to enter into this Agreement and agrees to all the terms specified herein.

Marisa Ramos, Ph.D. Chief, Office of Refugee Health	Date

Attachment A

Legal Authority for Use and Disclosure of Protected Data

I. Legal Authority for the Access, Collection, Use, Maintenance and Disclosure of Protected Data: The legal authority for CDPH to access, collect, use, maintain and disclose Protected Data, and for Data Recipient to receive and use Protected Data is as follows:

A. General Legal Authority:

1. California Information Practices Act:

a) California Civil Code section 1798.24, subdivision (e), provides in part as follows: "No agency may disclose any personal information in a manner that would link the information disclosed to the individual to whom it pertains unless the information is disclosed, as follows:

To a person, or to another agency where the transfer is necessary for the transferee agency to perform its constitutional or statutory duties, and the use is compatible with a purpose for which the information was collected...."

B. Specific Legal Authority:

1. Refugee Resettlement Program: Title 45 of the Code of Federal Regulations, Part 400.27, provides:

a. "Except for purposes directly connected with, and necessary to, the administration of the program, a State must ensure that no information about, or obtained from, an individual and in possession of any agency providing assistance or services to such individual under the plan, will be disclosed in a form identifiable with the individual without the individual's consent, or if the individual is a minor, the consent of his or her parent or guardian."

C. Health Insurance Portability and Accountability Act of 1996 (HIPAA) (2013) Authority:

1. CDPH HIPAA Status: CDPH is a "hybrid entity" for purposes of applicability of the federal regulations entitled "Standards for Privacy of Individually Identifiable Health Information" ("Privacy Rule") (45 C.F.R. Parts 160, 162, and 164) promulgated pursuant to the Health Insurance Portability and Accountability Act of 1996 (HIPAA) (42 U.S.C. §§ 1320d - 1320d-8) (as amended by Subtitle D Privacy, of the Health Information Technology for Economic and Clinical Health (HITECH) Act (Pub. L. 111–5, 123 Stat. 265–66).) Some of the CDPH programs that collect, use or disclose Protected

Data may be programs designated by CDPH as HIPAA-covered "health care components" of CDPH. (45 C.F.R. Part 164.504(c)(3)(iii).) All Protected Data of any CDPH health care component that is accessed, collected, used or disclosed as part of the RHEIS system fits within one or more of the exceptions set forth in subsection 3, below ("Protected Data Use and Disclosure Permitted by HIPAA").

2. Parties Are "Public Health Authorities": CDPH and Data Recipient are each a "public health authority" as that term is defined in the Privacy Rule. (45 C.F.R. Part 164.501; 164.512(b)(1)(i).)

3. Protected Data Use and Disclosure Permitted by HIPAA: To the extent a disclosure or use of Protected Data is a disclosure or use of "Protected Health Information" (PHI) of an individual, as that term is defined in Section 160.103 of Title 45, Code of Federal Regulations, the following Privacy Rule provisions apply to permit such Protected Data disclosure and/or use by CDPH and Data Recipient, without the consent or authorization of the individual who is the subject of the PHI:

    a) The HIPAA Privacy Rule creates a special rule for a subset of public health disclosures whereby HIPAA cannot preempt state law if, "[t]he provision of state law, including state procedures established under such law, as applicable, provides for the reporting of disease or injury, child abuse, birth, or death, or for the conduct of public health surveillance, investigation, or intervention." (45 C.F.R. Part 160.203(c) [HITECH Act, § 13421, sub. (a)].) [NOTE: See State laws and regulations listed in §§ IV.A and IV.B, above.];

    b) A covered entity may disclose PHI to a "public health authority" carrying out public health activities authorized by law; (45 C.F.R. Part 164.512(b).); and

    c) Other, non-public health-specific provisions of HIPAA may also provide the legal bases for all or specific Protected Data uses and disclosures.

Attachment B

Data Recipient Security Standards

1. **General Security Controls**

A. ***Confidentiality Statement***. All persons that will be working with Protected Data must sign a RHEIS confidentiality statement. (See Attachment D, RHEIS Confidentiality of Patient Information.) The statement must be signed by the workforce member prior to access to Protected Data. The statement must be renewed annually. The Data Recipient shall retain each person's written confidentiality statement for CDPH inspection for a period of three (3) years following contract termination.

C. ***Workstation/Laptop encryption***. All workstations and laptops that process and/or store Protected Data must be encrypted using a FIPS 140-2 certified algorithm, such as Advanced Encryption Standard (AES), with a 128bit key or higher. The encryption solution must be full disk unless approved by the CDPH Information Security Office.

D. ***Server Security***. Servers containing unencrypted Protected Data must have sufficient administrative, physical, and technical controls in place to protect that data, based upon a risk assessment/system security review.

E. ***Minimum Necessary***. Only the minimum necessary amount of Protected Data required to perform necessary business functions may be copied, downloaded, or exported.

F. ***Removable media devices***. All electronic files that contain Protected Data must be encrypted when stored on any removable media or portable device (i.e. USB thumb drives, floppies, CD/DVD, Blackberry, backup tapes etc.). Must be encrypted using a FIPS 140-2 certified algorithm, such as Advanced Encryption Standard (AES), with a 128bit key or higher.

G. ***Antivirus software***. All workstations, laptops and other systems that process and/or store Protected Data must install and actively use comprehensive anti-virus software solution with automatic updates scheduled at least daily.

H. ***Patch Management***. All workstations, laptops and other systems that process and/or store Protected Data must have security patches applied, with system reboot if necessary. There must be a documented patch management process which determines installation timeframe based on risk assessment and vendor recommendations. At a maximum, all applicable patches must be installed within 30 days of vendor release.

I. ***User IDs and Password Controls***. All users must be issued a unique user name for accessing Protected Data. Username must be promptly disabled, deleted, or the password changed upon the transfer or termination of an employee with knowledge of the password. Passwords are not to be shared. Must be at least eight characters. Must be a non-dictionary word. Must not be stored in readable format on the computer. Must be changed every 60 days. Must be changed if revealed or compromised. Must be composed of characters from at least three of the following four groups from the standard keyboard:

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

J. ***Data Sanitization***. All Protected Data must be sanitized using NIST Special Publication 800-88 standard methods for data sanitization when the CDPH PSCI is no longer needed.

2. **System Security Controls**

A. ***System Timeout***. The system must provide an automatic timeout, requiring re-authentication of the user session after no more than 20 minutes of inactivity.

B. ***Warning Banners***. All systems containing Protected Data must display a warning banner stating that data is confidential, systems are logged, and system use is for business purposes only. User must be directed to log off the system if they do not agree with these requirements.

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

D. ***Access Controls***. The system must use role based access controls for all user authentications, enforcing the principle of least privilege.

E. ***Transmission encryption***. All data transmissions of Protected Data outside the secure internal network must be encrypted using a FIPS 140-2 certified algorithm, such as Advanced Encryption Standard (AES), with a 128bit key or higher. Encryption can be end to end at the network level, or the data files containing Protected Data can be encrypted. This requirement pertains to any type of Protected Data in motion such as website access, file transfer, and e-mail.

F. ***Intrusion Detection***. All systems involved in accessing, holding, transporting, and protecting Protected Data that are accessible via the Internet must be protected by a comprehensive intrusion detection and prevention solution.

3. **Audit Controls**

A. ***System Security Review***. All systems processing and/or storing Protected Data must have at least an annual system risk assessment/security review which provides assurance that administrative, physical, and technical controls are functioning effectively and providing adequate levels of protection. Reviews shall include vulnerability scanning tools.

B. ***Log Reviews***. All systems processing and/or storing Protected Data must have a routine procedure in place to review system logs for unauthorized access.

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

4. **Business Continuity / Disaster Recovery Controls**

A. ***Disaster Recovery***. Data Recipient must establish a documented plan to enable continuation of critical business processes and protection of the security of electronic Protected Data in the event of an emergency. Emergency means any circumstance or situation that causes normal computer operations to become unavailable for use in performing the work required under this agreement for more than 24 hours.

B. ***Data Backup Plan***. Data Recipient must have established documented procedures to backup Protected Data to maintain retrievable exact copies of Protected Data. The plan must include a regular schedule for making backups, storing backups offsite, an inventory of backup media, and the amount of time to restore Protected Data should it be lost. At a minimum, the schedule must be a weekly full backup and monthly offsite storage of CDPH data.

5. **Paper Document Controls**

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

B. ***Escorting Visitors***. Visitors to areas where Protected Data is contained shall be escorted and Protected Data shall be kept out of sight while visitors are in the area.

C. ***Confidential Destruction***. Protected Data must be disposed of through confidential means, using NIST Special Publication 800-88 standard methods for data sanitization when the Protected Data is no longer needed.

D. ***Removal of Data***. Protected Data must not be removed from the premises of the Data Recipient except with express written permission of CDPH.

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

F. ***Mailing***. Protected Data shall only be mailed using secure methods. Large volume mailings of Protected Data shall be by a secure, bonded courier with signature required on receipt. Disks and other transportable media sent through the mail must be encrypted with a CDPH approved solution, such as a solution using a vendor product specified on the CSSI.

Attachment C

Agreement by Employee/Data Recipient to Comply with Confidentiality Requirements

Summary of Statutes Pertaining to Confidential Public Health Records and Penalties for Disclosure

All HIV/AIDS case reports and any information collected or maintained in the course of surveillance-related activities that may directly or indirectly identify an individual are considered *confidential public health record(s)* under California Health and Safety Code (HSC), Section 121035(c) and must be handled with the utmost confidentiality. Furthermore, HSC §121025(a) prohibits the disclosure of HIV/AIDS-related public health records that contain any personally identifying information to any third party, unless authorized by law for public health purposes, or by the written consent of the individual identified in the record or his/her guardian/conservator. Except as permitted by law, any person who negligently discloses information contained in a confidential public health record to a third party is subject to a civil penalty of up to $5,000 plus court costs, as provided in HSC §121025(e)(1). Any person who willfully or maliciously discloses the content of a public health record, except as authorized by law, is subject to a civil penalty of $5,000-$25,000 plus court costs as provided by HSC §121025(e)(2). Any willful, malicious, or negligent disclosure of information contained in a public health record in violation of state law that results in economic, bodily, or psychological harm to the person named in the record is a misdemeanor, punishable by imprisonment for a period of up to one year and/or a fine of up to $25,000 plus court costs (HSC §121025(e)(3)). Any person who is guilty of a confidentiality infringement of the foregoing type may be sued by the injured party and shall be personally liable for all actual damages incurred for economic, bodily, or psychological harm as a result of the breach (HSC §121025(e)(4)). Each disclosure in violation of California law is a separate, actionable offense (HSC §121025(e)(5)).

Because an assurance of case confidentiality is the foremost concern of the California Department of Public Health, Office of AIDS (CDPH/OA), any actual or potential breach of confidentiality shall be immediately reported. In the event of any suspected breach, staff shall immediately notify the director or supervisor of the local health department's HIV/AIDS surveillance unit who in turn shall notify the CDPH/OA Surveillance Section Chief or designee. CDPH/OA, in conjunction with the local health department and the local health officer shall promptly investigate the suspected breach. Any evidence of an actual breach shall be reported to the law enforcement agency that has jurisdiction.

Employee Confidentiality Pledge

I recognize that in carrying out my assigned duties, I may obtain access to private information about persons diagnosed with HIV or AIDS that was provided under an assurance of confidentiality. I understand that I am prohibited from disclosing or otherwise releasing any personally identifying information, either directly or indirectly, about any individual named in any HIV/AIDS confidential public health record. Should I be responsible for any breach of confidentiality, I understand that civil and/or criminal penalties may be brought against me. I acknowledge that my responsibility to ensure the privacy of protected health information contained in any electronic records, paper documents, or verbal communications to which I may gain access shall not expire, even after my employment or affiliation with the Department has terminated.

By my signature, I acknowledge that I have read, understand, and agree to comply with the terms and conditions above.

_____	_____	_____
Employee name (print)	Employee Signature	Date
_____	_____	_____
Supervisor name (print)	Supervisor Signature	Date

_____
Name of Employer

P L E A S E R E T A I N A C O P Y O F T H I S D O C U M E N T F O R Y O U R R E C O R D S.

Attachment D

California Department of Public Health
Office of Refugee Health
Refugee Health Electronic Information System (RHEIS)

CONFIDENTIALITY OF PATIENT INFORMATION

On behalf of the State of California Department of Public Health, Office of Refugee Health (CDPH/ORH), you have been authorized to work with confidential medical information and individual medical records. Such information is not to be shared with unauthorized employees, family, friends and/or acquaintances. It is illegal and unethical to disclose any information including:

- Record, case or medical identification number
- Discuss patient identity, name, date of birth, gender, etc.
- Discuss clinical activity of test results
- Discuss case with other employees
- Disclosure of medical insurance or method of payment
- Answer telephone inquiries
- Sharing or transfer of medical records physically, electronically or by mail

As an authorized RHEIS user, you agree to access the RHEIS system only for performance of legitimate governmental business. RHEIS users must ensure the integrity, security, and confidentiality of RHEIS data and permit appropriate disclosure and use of such data only as permitted by law.

You agree that you are responsible for complying with your County's Privacy and Information Security Policies when accessing the RHEIS system. You are also responsible for the confidentiality and security of your selected password. Never leave your computer terminal or workstation unattended when using RHEIS. The following preventive measures must be taken to protect your password:

- Keep your password a secret to yourself.
- Shared passwords are strictly prohibited.
- Passwords should be changed on a regular basis.
- RHEIS will also prompt you to change you password every 60 days.
- Do not write or paste your password on your terminal.
- Do not automate your password in a data file, log-on script, or macro.

CDPH/ORH reserves the right to terminate the RHEIS account of any user at any time.

I, _____ have read the above and acknowledge my responsibility to conform to this policy.
(*Print name of RHEIS user*)

County _____

Work Address _____
(Street) *(City)* *(State)* *(Zip)*

Work Number: _____ Email: _____

_____ _____
Employee Signature Date

_____ _____
County RHAP Coordinator Signature Date

***** If the County RHAP Coordinator authorized you to be a RHEIS user and you are a non-RHAP staff member, then the County RHAP will be responsible in providing RHEIS technical service to you.**

California Refugee Health Assessment

1. Identification

Alien Number
or VOT HHS Tracking Number

Demographic Data

File Number

County Medical Record Number

Last Name

First Name

☐ Male ☐ Female
☐ Female to Male Transgender
☐ Male to Female Transgender

/ / ☐ Approximate
Date of Birth (MM/DD/YYYY)

Email

Current Address

Street

Apartment #

City

ZIP Code

Contact Phone Numbers

Home

Cell

2. Arrival Data

Entry Status

Is a copy of I-94 or other eligibility document in file? Yes ☐ Not applicable ☐

☐ Refugee

/ /
U.S. Arrival Date (I-94)
(MM/DD/YYYY)

☐ Primary
☐ Secondary to State

Specify State

/ /
Date to CA
(MM/DD/YYYY)

☐ Asylee

/ /
U.S. Arrival/
Adjudication Date
(MM/DD/YYYY)

☐ Inside U.S.

Detention center
name, if any

☐ Outside U.S.

☐ Parolee

/ /
Paroled Date
(MM/DD/YYYY)

☐ Cuba
☐ Haiti

☐ Victim of trafficking

/ /
Certification Date
(MM/DD/YYYY)

☐ Other

/ /
U.S. Arrival Date
(MM/DD/YYYY)

☐ Special Immigrant Visa
☐ Amerasian
☐ Other

Voluntary Resettlement Agency Information

Voluntary Resettlement Agency Name

County

☐ No Voluntary Agency

City

State

ZIP Code

Medi-Cal

Has Medi-Cal? ☐ Yes **Medi-Cal Number** ☐ Pending / / Application Date (MM/DD/YYYY) ☐ No Reason

Interpreter

Was an interpreter used? ☐ Yes ☐ No

If yes, what type ☐ In-Person ☐ Video ☐ Phone ☐ Other

3. Demographics

Country of Birth and Ethnicity

Country of Birth _____ Ethnicity _____

Mother's Country of Birth _____

Languages

Primary _____

Secondary _____

Education and Occupation

Not applicable ☐

Years of Education _____ Previous or Current Occupation _____

Residing Country Prior to U.S. (last 2 years)

Not applicable ☐

Country (most recent first)	Refugee Camp (if applicable)	Length of stay		
		Years	Months	Days

4. Assessment Disposition

Assessment Status

☐ Started

Date Started (MM/DD/YYYY) ___/___/_____

Date of Final Visit (MM/DD/YYYY) ___/___/_____

☐ Fully completed

☐ Partially completed

☐ Partially completed ☐ Not started

Reason:

☐ Used other provider
☐ Moved to _____
☐ Unable to locate
☐ Declined
☐ Medi-Cal eligibility issue _____
☐ Deceased
☐ Did not keep appointment
☐ Other _____

5. Overseas Medical Exam (DS-2053 or DS-2054)

Form DS-2053 or DS-2054

DS-2053 or DS-2054 Reviewed? ☐ Yes ☐ Not available, reason _____ ☐ Not applicable

Classifications

☐ No apparent defect, disease, or disability

Class A Conditions (Check all that apply)

☐ TB, active, infectious
☐ Syphilis, untreated
☐ Chancroid, untreated
☐ Gonorrhea, untreated
☐ Granuloma inguinale, untreated
☐ Lymphogranuloma venereum, untreated
☐ Hansen's disease, lepromatous, or multibacilliary
☐ Addiction or abuse of specific substance without harmful behavior
☐ Any physical or mental disorder with harmful behavior or history of such behavior likely to recur

Class B Conditions (Check all that apply)

☐ TB, active, noninfectious (DS-2053)
☐ TB, inactive (DS-2053)
☐ TB Classification (DS-2054)
  ☐ B1 TB, Pulmonary
  ☐ B1 TB, Extrapulmonary
  ☐ B2 TB, LTBI Evaluation
  ☐ B3 TB, Contact Evaluation
  ☐ Other _____
☐ Syphilis (with residual deficit), treated within the last year
☐ Other sexually transmitted infections, treated within last year
☐ Current pregnancy
☐ Hansen's disease, prior treatment
☐ Hansen's disease, tuberculoid, borderline, or paucibacillary
☐ Sustained, full remission of addiction or abuse of specific substances
☐ Any physical or mental disorder with harmful behavior or history of such behavior likely to recur
☐ Other _____

5. Overseas Medical Exam (Continued)

Pre-Departure Treatments

☐ Intestinal parasites

- ☐ No treatment
- ☐ Praziquantel
- ☐ Albendazole
- ☐ Other _____
- ☐ Ivermectin

☐ Anti-Malaria

- ☐ No treatment
- ☐ Quinine
- ☐ Artemether-Lumefantrine
- ☐ Other _____
- ☐ Amodiaquine-Artesunate

6. Immunizations

	Overseas Immunization Status					Updated in RHAP Clinic				Referred Out	
	Completed	Not started	Series started	No records provided	Not applicable	Yes	No	Declined	Not applicable	Yes*	Not applicable
Diphtheria, Tetanus, and Pertussis (DPT/DTaP/DT/Tdap)	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Tetanus (Td)	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Haemophilus influenzae type b (Hib)	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Polio (IPV/OPV)	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Hepatitis B (HBV)	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Hepatitis A (HAV)	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Measles, Mumps, Rubella (MMR)	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Varicella (VAR)	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Rotavirus (RV1/RV5)	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Meningococcal (MCV4)	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Influenza	☐	☐		☐	☐	☐	☐	☐	☐	☐	☐
Pneumococcal	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Other _____	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Other _____	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Other _____	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

*If referred out, where? _____

7. Tuberculosis

Overseas Chest X-Ray Findings

__/__/____
X-Ray Date (MM/DD/YYYY)

☐ Normal ☐ Abnormal ☐ Not Available ☐ Not Applicable

U.S. IGRA

☐ IGRA

__/__/____
Date Drawn (MM/DD/YYYY)

☐ QFT Results: ☐ + ☐ - ☐ Indeterminate

QFT IU ____

☐ TSpot Results: ☐ + ☐ - ☐ Borderline

Spots ____ A Spots ____ B Spots ____

☐ No IGRA

Reason:

☐ Moved to ____
☐ Did not keep appointment
☐ Deceased
☐ Insufficient blood draw
☐ Lost to follow-up
☐ Declined
☐ TST Performed
☐ Other ____

U.S. TST

☐ TST Placed

__/__/____
Date Placed (MM/DD/YYYY)

__/__/____
Date Read (MM/DD/YYYY)

Results: ☐ + ☐ - ☐ Did not return for reading

____mm
Induration

☐ No TST

Reason:

☐ Moved to ____
☐ Lost to follow-up
☐ Did not keep appointment
☐ IGRA performed
☐ Declined
☐ Deceased
☐ Other ____

U.S. Chest X-Ray

☐ U.S. Chest X-Ray Performed

__/__/____
Date (MM/DD/YYYY)

Result:

☐ Normal
☐ Abnormal (consistent with TB)
☐ Abnormal (NOT consistent with TB)
☐ Unavailable, reason ____

☐ No U.S. Chest X-Ray Performed

Reason:

☐ Moved to ____
☐ Lost to follow-up
☐ Did not keep appointment
☐ Declined
☐ Deceased
☐ Pregnancy
☐ Not applicable
☐ Other ____

Disposition

☐ Completed

Result:

☐ TB Class 0 (No TB exposure, not infected)
☐ TB Class I (TB exposure, no infection)
☐ TB Class II (TB infection, no disease)
☐ TB Class III (TB, clinically active)
☐ TB Class IV (TB, not clinically active)

☐ TB Class V (TB suspected, pending final diagnosis)

Reason for retaining TB V classification:

☐ Moved to ____
☐ Lost to follow-up
☐ Work-up in progress
☐ Deceased
☐ Other ____

☐ Not Completed

Reason:

☐ Moved to ____
☐ Lost to follow-up
☐ Did not keep appointment
☐ Declined
☐ Deceased
☐ Other ____

LTBI Treatment

☐ LTBI Treatment

__/__/____
Started Date (MM/DD/YYYY)

__/__/____
Stopped Date (MM/DD/YYYY)

Reason LTBI treatment stopped:

☐ Treatment completed
☐ Moved to ____
☐ Lost to follow-up
☐ Did not keep appointment
☐ Declined
☐ Deceased
☐ Active TB developed
☐ Changed to outside provider
☐ Adverse effect of medicine
☐ Other ____

☐ No LTBI Treatment

Reason:

☐ Moved to ____
☐ Lost to follow-up
☐ Did not keep appointment
☐ Declined
☐ Deceased
☐ Pregnancy
☐ Changed to outside provider
☐ Patient's age
☐ Medical contraindication
☐ Prior adequate treatment
☐ Other ____

Comments

8. Laboratory Tests (Refer to RHAP protocol for specific guidelines)

If a lab test is not completed, provide reason in section 17.

CBC with Differential	Hemoglobin	☐ Normal	☐ Abnormal	Value _____	☐ Not applicable
	Hematocrit	☐ Normal	☐ Abnormal	Value _____	☐ Not applicable
	Absolute Eosinophil Count	☐ Normal	☐ Abnormal	Value _____	☐ Not applicable
Chlamydia		☐ Positive	☐ Negative	☐ Not applicable	
Fecal Occult Blood		☐ Positive	☐ Negative	☐ Not applicable	
Hepatitis B - HBsAg		☐ Reactive	☐ Non-reactive	☐ Not applicable	
Hepatitis B - Anti-HBc		☐ Reactive	☐ Non-reactive	☐ Not applicable	
Hepatitis B - Anti-HBs		☐ Reactive	☐ Non-reactive	☐ Not applicable	
Hepatitis C - Anti HCV		☐ Reactive	☐ Non-reactive	☐ Not applicable	
HIV		☐ Positive ☐ Type I ☐ Type II	☐ Negative	☐ Inconclusive	☐ Declined ☐ NA
Lipid Panel ☐ Random ☐ Fasting	Total Cholesterol	☐ Elevated	☐ Not elevated	☐ Not applicable	Value _____
	HDL	☐ Elevated	☐ Not elevated	☐ Not applicable	Value _____
	LDL	☐ Elevated	☐ Not elevated	☐ Not applicable	Value _____
	Triglycerides	☐ Elevated	☐ Not elevated	☐ Not applicable	Value _____
Malaria		☐ Positive	☐ Negative	☐ Not applicable	
Pregnancy Test ☐ Urine ☐ Serum		☐ Positive __/__/____ EDC Date (MM/DD/YYYY)	☐ Negative	☐ Not applicable	☐ Currently pregnant
Serum Glucose ☐ Random ☐ Fasting		☐ Elevated	☐ Not elevated	☐ Not applicable	Value _____
Blood Lead		☐ Elevated	☐ Not elevated	☐ Not applicable	Value _____
Syphilis VDRL or RPR		☐ Reactive*	☐ Nonreactive	☐ Not applicable	Value _____
*If Reactive, which test ☐ FTA-ABS ☐ TP-PA ☐ TP-MHA		☐ Positive	☐ Negative	☐ Not applicable	Value _____

Parasitic Infection	Value	Findings / Treated
Stool Sample 1	☐ Positive ☐ Negative ☐ Not Applicable	Parasite 1 _____ ☐ Yes ☐ No, reason _____ Parasite 2 _____ ☐ Yes ☐ No, reason _____ Parasite 3 _____ ☐ Yes ☐ No, reason _____ Parasite 4 _____ ☐ Yes ☐ No, reason _____ Parasite 5 _____ ☐ Yes ☐ No, reason _____
Stool Sample 2	☐ Positive ☐ Negative ☐ Not Applicable	Parasite 1 _____ ☐ Yes ☐ No, reason _____ Parasite 2 _____ ☐ Yes ☐ No, reason _____ Parasite 3 _____ ☐ Yes ☐ No, reason _____ Parasite 4 _____ ☐ Yes ☐ No, reason _____ Parasite 5 _____ ☐ Yes ☐ No, reason _____
Serum Strongyloides	☐ Positive ☐ Negative ☐ Not Applicable	☐ Yes ☐ No, reason _____
Serum Schistosomiasis	☐ Positive ☐ Negative ☐ Not Applicable	☐ Yes ☐ No, reason _____

9. Patient Medical History

Medical Condition	No History	Check All that Apply	If applicable, what type(s)	Taking Medications for Condition
Allergies	☐	☐ Current ☐ Past		☐ Yes, specify ☐ No
Anemia	☐	☐ Current ☐ Past		☐ Yes, specify ☐ No
Cancer	☐	☐ Current ☐ Past		☐ Yes, specify ☐ No
Cardiovascular Dz	☐	☐ Current ☐ Past		☐ Yes, specify ☐ No
Diabetes Mellitus	☐	☐ Current ☐ Past		☐ Yes, specify ☐ No
Epilepsy	☐	☐ Current ☐ Past		☐ Yes, specify ☐ No
Hepatitis	☐	☐ Current ☐ Past		☐ Yes, specify ☐ No
High Cholesterol	☐	☐ Current ☐ Past		☐ Yes, specify ☐ No
Hypertension	☐	☐ Current ☐ Past		☐ Yes, specify ☐ No
Kidney Dz	☐	☐ Current ☐ Past		☐ Yes, specify ☐ No
Liver Dz	☐	☐ Current ☐ Past		☐ Yes, specify ☐ No
Lung Dz	☐	☐ Current ☐ Past		☐ Yes, specify ☐ No
Mental/Emotional	☐	☐ Current ☐ Past		☐ Yes, specify ☐ No
Stroke	☐	☐ Current ☐ Past		☐ Yes, specify ☐ No
Surgery(ies)	☐	☐ Current ☐ Past		☐ Yes, specify ☐ No
Tuberculosis	☐	☐ Current ☐ Past		☐ Yes, specify ☐ No
Thyroid Dz	☐	☐ Current ☐ Past		☐ Yes, specify ☐ No
Other (specify)	☐	☐ Current ☐ Past		☐ Yes, specify ☐ No
Other (specify)	☐	☐ Current ☐ Past		☐ Yes, specify ☐ No

Supplements (Vitamins, Herbs, Etc.)

Are you taking supplements? ☐ Yes ☐ No

_____
If yes, supplements taken

Menstrual History

Not applicable (pre-puberty) ☐

☐ Menstruating ___/___/_____
Date of LMP
(MM/DD/YYYY)

☐ Menopausal _____
Age stopped menstruating

Pregnancy History

Not applicable (pre-puberty) ☐

Gravida	Para	SAB	TAB
_____	_____	_____	_____

Female Genital Cutting

Declined ☐

Female genital cutting ☐ Yes ☐ No

☐ Clitoridectomy ☐ Infibulation ☐ Excision
☐ Other _____ ☐ Unknown

10. Family Medical History

Medical Condition	If applicable, what type(s)	
Cancer	☐ No history	☐ Mother ☐ Father ☐ Maternal grandmother ☐ Maternal grandfather ☐ Paternal grandmother ☐ Paternal grandfather ☐ Sibling(s)
Kidney Dz	☐ No history	☐ Mother ☐ Father ☐ Maternal grandmother ☐ Maternal grandfather ☐ Paternal grandmother ☐ Paternal grandfather ☐ Sibling(s)
Cardiovascular Dz	☐ No history	☐ Mother ☐ Father ☐ Maternal grandmother ☐ Maternal grandfather ☐ Paternal grandmother ☐ Paternal grandfather ☐ Sibling(s)
Lung Dz	☐ No history	☐ Mother ☐ Father ☐ Maternal grandmother ☐ Maternal grandfather ☐ Paternal grandmother ☐ Paternal grandfather ☐ Sibling(s)
Diabetes Mellitus	☐ No history	☐ Mother ☐ Father ☐ Maternal grandmother ☐ Maternal grandfather ☐ Paternal grandmother ☐ Paternal grandfather ☐ Sibling(s)
Mental/Emotional	☐ No history	☐ Mother ☐ Father ☐ Maternal grandmother ☐ Maternal grandfather ☐ Paternal grandmother ☐ Paternal grandfather ☐ Sibling(s)
Hepatitis	☐ No history	☐ Mother ☐ Father ☐ Maternal grandmother ☐ Maternal grandfather ☐ Paternal grandmother ☐ Paternal grandfather ☐ Sibling(s)
Stroke	☐ No history	☐ Mother ☐ Father ☐ Maternal grandmother ☐ Maternal grandfather ☐ Paternal grandmother ☐ Paternal grandfather ☐ Sibling(s)
High Cholesterol	☐ No history	☐ Mother ☐ Father ☐ Maternal grandmother ☐ Maternal grandfather ☐ Paternal grandmother ☐ Paternal grandfather ☐ Sibling(s)
Thyroid Dz	☐ No history	☐ Mother ☐ Father ☐ Maternal grandmother ☐ Maternal grandfather ☐ Paternal grandmother ☐ Paternal grandfather ☐ Sibling(s)
Hypertension	☐ No history	☐ Mother ☐ Father ☐ Maternal grandmother ☐ Maternal grandfather ☐ Paternal grandmother ☐ Paternal grandfather ☐ Sibling(s)
Tuberculosis	☐ No history	☐ Mother ☐ Father ☐ Maternal grandmother ☐ Maternal grandfather ☐ Paternal grandmother ☐ Paternal grandfather ☐ Sibling(s)

11. Lifestyle Assessment (13 years of age and older)

Health Behaviors

Declined to answer ☐ Not applicable ☐

Exercise

During the last 30 days, did you exercise?

☐ Yes – Days per week _____ Minutes per day _____

☐ No

Smoking

1. Have you ever smoked?

☐ Yes, age started _____

☐ No (skip to question 4)

2. Do you now smoke?

☐ Every day

☐ Some days

☐ No, age stopped _____

3. On average, how many or how long do/did you smoke a day?

# of Cigarettes _____

# of Pipes _____

# of Cigars _____

# of Other Tobacco _____

# of minutes per day of Hookah, Shisha, Ḡalyān, Narghile or Chillin _____

4. Is smoking ever allowed inside your home?

☐ Yes, # of hours per day _____

☐ No

Alcohol

1. During the past 30 days, have you had at least one alcoholic drink?

☐ Yes

☐ No (skip questions 2 and 3)

2. During the past 30 days, how many days per month did you have at least one alcoholic drink?

# of Days/Month _____

3. During the past 30 days, on the days when you drank, about how many drinks did you drink on the average?

# of Wine Drinks _____
(3-5 oz)

# of Beer Drinks _____
(10-12 oz or 1 bottle)

# of Hard Liquor Drinks _____
(1-1.5 oz)

Health Education

Was health education provided on health behaviors (exercise, diet/nutrition, smoking, and alcohol)?

☐ Yes – ☐ Written ☐ Verbal

☐ No

12. Mental Health (16 years of age and older. Refer to RHAP protocol for guidelines & scoring rubric.)

PTSD Screening

Declined to answer ☐ Not applicable ☐

In your life, have you ever had any experience that was so frightening, horrible, or upsetting that, in the past month, you:

	Yes	No
1. Have had nightmares about it or thought about it when you did not want to?	☐	☐
2. Tried hard not to think about it or went out of your way to avoid situations that reminded you of it?	☐	☐
3. Were constantly on guard, watchful, or easily startled?	☐	☐
4. Felt numb or detached from others, activities, or your surroundings?	☐	☐

Generalized Anxiety Disorder Screening

Declined to answer ☐ Not applicable ☐

Over the past 2 weeks, how often have you been bothered by the following problems?

	Not at all (0)	Several days (1)	More than half of the days (2)	Nearly every day (3)
1. Feeling nervous, anxious, or on edge.	☐	☐	☐	☐
2. Not being able to stop or control worrying.	☐	☐	☐	☐

Depression

Declined to answer ☐ Not applicable ☐

Over the past 2 weeks, how often have you been bothered by the following problems?

	Not at all (0)	Several days (1)	More than half of the days (2)	Nearly every day (3)
1. Little interest or pleasure doing things.	☐	☐	☐	☐
2. Feeling down, depressed, or hopeless.	☐	☐	☐	☐

13. Traumatic Events (16 years of age and older. Refer to RHAP protocol for guidelines & scoring rubric.)

Trauma

Declined to answer ☐ Not applicable ☐

Listed below are a number of difficult or stressful things that sometimes happen to people. For each event tell me if: a) it *happened to you* personally, b) you *witnessed it* happen to someone else, c) you *learned about it* happening to someone close to you, d) it *doesn't apply* to you. Be sure to consider your entire life (growing up as well as adulthood) as I go through the list of events.

Check all that apply:	Happened to me	Witnessed it	Learned about it	Doesn't apply
1. Physical assault (for example, being attacked, hit, slapped, kicked, or beaten up)	☐	☐	☐	☐
2. Assault with a weapon (for example, being shot, stabbed, threatened with a knife, gun, bomb, or land mine)	☐	☐	☐	☐
3. Sexual assault (for example, rape, attempted rape, made to perform any type of sexual act through force or threat of harm)	☐	☐	☐	☐
4. Captivity (for example, being kidnapped, abducted, held hostage, prisoner of war, or forced labor)	☐	☐	☐	☐
5. Sudden, violent death of a family member (for example, homicide, or suicide)	☐	☐	☐	☐
6. Serious injury, harm, or death you caused to someone else	☐	☐	☐	☐
7. Any other very stressful event or experience which caused you to experience intense fear	☐	☐	☐	☐
8. Sudden move or loss of home and possessions	☐	☐	☐	☐

Persecution

Declined to answer ☐ Not applicable ☐

Have you experienced any type of persecution? ☐ Yes ☐ No

If yes, check all that apply: ☐ Religious ☐ Political ☐ Ethnic ☐ Reproductive choices ☐ Military service escapee ☐ Other _____

14. Vital Signs / Measurements

Vital Signs

Temperature _____ ☐ ˚F ☐ ˚C Pulse _____

B/P (6 years +) **1.** _____ / _____ **2.** _____ / _____ **3.** _____ / _____
systolic / diastolic; systolic / diastolic; systolic / diastolic

Measurements

Height _____ ☐ inches ☐ cm Weight _____ ☐ lbs ☐ kg Head circumference _____ ☐ inches ☐ cm
(2 years and under)

Vision (6 years +) Glasses/contact lenses worn ☐ Yes ☐ No

_____ Left _____ Right _____ Both

Difficulty hearing (6 years +) ☐ Yes ☐ No

15. Physical Exam

Findings						Comments
Abdomen	☐ Normal	☐ Abnormal	☐ Declined	☐ Deferred	☐ Not appropriate	
Breast	☐ Normal	☐ Abnormal	☐ Declined	☐ Deferred	☐ Not appropriate	
Ears	☐ Normal	☐ Abnormal	☐ Declined	☐ Deferred	☐ Not appropriate	
Extremities	☐ Normal	☐ Abnormal	☐ Declined	☐ Deferred	☐ Not appropriate	
Eyes	☐ Normal	☐ Abnormal	☐ Declined	☐ Deferred	☐ Not appropriate	
Genital	☐ Normal	☐ Abnormal	☐ Declined	☐ Deferred	☐ Not appropriate	
Head	☐ Normal	☐ Abnormal	☐ Declined	☐ Deferred	☐ Not appropriate	
Heart	☐ Normal	☐ Abnormal	☐ Declined	☐ Deferred	☐ Not appropriate	
Lungs	☐ Normal	☐ Abnormal	☐ Declined	☐ Deferred	☐ Not appropriate	
Lymph Nodes	☐ Normal	☐ Abnormal	☐ Declined	☐ Deferred	☐ Not appropriate	
Mouth	☐ Normal	☐ Abnormal	☐ Declined	☐ Deferred	☐ Not appropriate	
Neurologic	☐ Normal	☐ Abnormal	☐ Declined	☐ Deferred	☐ Not appropriate	
Nose	☐ Normal	☐ Abnormal	☐ Declined	☐ Deferred	☐ Not appropriate	
Rectal	☐ Normal	☐ Abnormal	☐ Declined	☐ Deferred	☐ Not appropriate	
Skin	☐ Normal	☐ Abnormal	☐ Declined	☐ Deferred	☐ Not appropriate	
Throat	☐ Normal	☐ Abnormal	☐ Declined	☐ Deferred	☐ Not appropriate	
Other	☐ Normal	☐ Abnormal	☐ Declined	☐ Deferred	☐ Not appropriate	

Physical exam was not completed, why?

☐ Declined ☐ Other _____

16. Diagnosis

Findings

☐ No overseas findings, and no U.S. findings.

ICD10	Diagnosis	Findings	Follow-up	Date Seen by Outside Provider (optional)
		☐ Overseas findings ☐ New, U.S. findings	☐ Problem addressed or treated at refugee clinic ☐ Problem referred to primary care ☐ Problem referred to specialty clinic, type: ________ ☐ Problem referred to emergency care ☐ Follow-up for this problem not currently available under current medical insurance (such as optometry, dental, etc.)	/ / Date (MM/DD/YYYY) Check one: ☐ Lost to follow-up ☐ Declined follow-up
		☐ Overseas findings ☐ New, U.S. findings	☐ Problem addressed or treated at refugee clinic ☐ Problem referred to primary care ☐ Problem referred to specialty clinic, type: ________ ☐ Problem referred to emergency care ☐ Follow-up for this problem not currently available under current medical insurance (such as optometry, dental, etc.)	/ / Date (MM/DD/YYYY) Check one: ☐ Lost to follow-up ☐ Declined follow-up
		☐ Overseas findings ☐ New, U.S. findings	☐ Problem addressed or treated at refugee clinic ☐ Problem referred to primary care ☐ Problem referred to specialty clinic, type: ________ ☐ Problem referred to emergency care ☐ Follow-up for this problem not currently available under current medical insurance (such as optometry, dental, etc.)	/ / Date (MM/DD/YYYY) Check one: ☐ Lost to follow-up ☐ Declined follow-up
		☐ Overseas findings ☐ New, U.S. findings	☐ Problem addressed or treated at refugee clinic ☐ Problem referred to primary care ☐ Problem referred to specialty clinic, type: ________ ☐ Problem referred to emergency care ☐ Follow-up for this problem not currently available under current medical insurance (such as optometry, dental, etc.)	/ / Date (MM/DD/YYYY) Check one: ☐ Lost to follow-up ☐ Declined follow-up
		☐ Overseas findings ☐ New, U.S. findings	☐ Problem addressed or treated at refugee clinic ☐ Problem referred to primary care ☐ Problem referred to specialty clinic, type: ________ ☐ Problem referred to emergency care ☐ Follow-up for this problem not currently available under current medical insurance (such as optometry, dental, etc.)	/ / Date (MM/DD/YYYY) Check one: ☐ Lost to follow-up ☐ Declined follow-up
		☐ Overseas findings ☐ New, U.S. findings	☐ Problem addressed or treated at refugee clinic ☐ Problem referred to primary care ☐ Problem referred to specialty clinic, type: ________ ☐ Problem referred to emergency care ☐ Follow-up for this problem not currently available under current medical insurance (such as optometry, dental, etc.)	/ / Date (MM/DD/YYYY) Check one: ☐ Lost to follow-up ☐ Declined follow-up
		☐ Overseas findings ☐ New, U.S. findings	☐ Problem addressed or treated at refugee clinic ☐ Problem referred to primary care ☐ Problem referred to specialty clinic, type: ________ ☐ Problem referred to emergency care ☐ Follow-up for this problem not currently available under current medical insurance (such as optometry, dental, etc.)	/ / Date (MM/DD/YYYY) Check one: ☐ Lost to follow-up ☐ Declined follow-up

Is VOLAG follow-up assistance needed?

☐ Yes ☐ No

17. Reason for Not Completing Any Screening Requirements

18. Signatures

Physical Exam Performed By

Name (print) | Signature | Date (MM/DD/YYYY) / /

Physical Exam Reviewed By

☐ Same as above

Name (print) | Signature | Date (MM/DD/YYYY) / /

Intake Interviewer 1

Name (print) | Signature | Date (MM/DD/YYYY) / /

Intake Interviewer 2

Name (print) | Signature | Date (MM/DD/YYYY) / /

Other Provider

Name (print) | Signature | Date (MM/DD/YYYY) / /

Role