

CONTRACT
BETWEEN
COUNTY OF ORANGE
AND
ALL FOR KIDS ORGANIZATION
AND
OLIVE CREST
AND
HUMAN OPTIONS, INC.
FOR THE PROVISION OF
FAMILY RESOURCE CENTER SERVICES

This Contract is by and between the COUNTY OF ORANGE, hereinafter referred to as “COUNTY,” and All For Kids Organization, a California private non-profit corporation, and Olive Crest, a California private non-profit corporation, and Human Options, Inc., a California private non-profit corporation, hereinafter referred to as “Oak View Family Resource Center” or “CONTRACTOR.” This Contract shall be administered by the County of Orange Social Services Agency Director or designee, hereinafter referred to as “ADMINISTRATOR.”

W I T N E S S E T H:

WHEREAS, COUNTY issued a Request For Proposal for Family Resource Center Services in 2024;

WHEREAS, COUNTY desires to contract with CONTRACTOR for the provision of Family Resource Center Services in Orange County;

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

WHEREAS, such services are authorized and provided pursuant to the Adoptions and Safe Families Act of 1997 (Public Law 105-89), California Welfare and Institutions Code

Sections 16600-16605 and 15610-15771, All County Letter (ACL) No. 01-20, ACL No. 03-12, ACL No. 14.12, and the Child and Family Services Improvement and Innovation Act; and

ACCORDINGLY, THE PARTIES AGREED AS FOLLOWS:

TABLE OF CONTENTS

1.	TERM.....	5
2.	ALTERATION OF TERMS	5
3.	STATUS OF CONTRACTOR.....	5
4.	DESCRIPTION OF SERVICES.....	6
5.	LICENSES AND STANDARDS.....	6
6.	DELEGATION AND ASSIGNMENT/CHANGE OF OWNERSHIP.....	7
7.	SUBCONTRACTS	8
8.	FORM OF BUSINESS ORGANIZATION/NAME CHANGE.....	9
9.	NON-DISCRIMINATION.....	10
10.	NOTICES	14
11.	NOTICE OF DELAYS	14
12.	INDEMNIFICATION.....	15
13.	INSURANCE.....	15
14.	NOTIFICATION OF LITIGATION, INCIDENTS, CLAIMS, OR SUITS	20
15.	CONFLICT OF INTEREST	21
16.	ANTI-PROSELYTISM PROVISION	21
17.	SUPPLANTING GOVERNMENT FUNDS.....	21
18.	EQUIPMENT.....	22
19.	BREACH SANCTIONS	23
20.	PAYMENTS	24
21.	OVERPAYMENTS	26
22.	OUTSTANDING DEBT.....	26
23.	FINAL REPORT.....	26
24.	INDEPENDENT AUDIT.....	26
25.	RECORDS, INSPECTIONS, AND AUDITS.....	27
26.	PERSONNEL DISCLOSURE	29
27.	EMPLOYMENT ELIGIBILITY VERIFICATION.....	32
28.	CHILD AND DEPENDENT ADULT/ELDER ABUSE REPORTING.....	32
29.	NOTICE TO EMPLOYEES REGARDING THE SAFELY SURRENDERED BABY LAW	33
30.	CONFIDENTIALITY	33
31.	SECURITY	34
32.	COPYRIGHT ACCESS	34
33.	WAIVER.....	34
34.	SERVICES DURING EMERGENCY AND/OR DISASTER	35
35.	PUBLICITY, LITERATURE, ADVERTISEMENTS AND SOCIAL MEDIA.....	36
36.	REPORTS	37
37.	ENERGY EFFICIENCY STANDARDS.....	37
38.	ENVIRONMENTAL PROTECTION STANDARDS	37
39.	CERTIFICATION AND DISCLOSURE REGARDING PAYMENTS TO INFLUENCE CERTAIN FEDERAL TRANSACTIONS	38
40.	POLITICAL ACTIVITY	39
41.	TERMINATION PROVISIONS.....	39
42.	COOPERATIVE CONTRACT.....	41
43.	GOVERNING LAW AND VENUE.....	42
44.	SIGNATURE IN COUNTERPARTS.....	42

ATTACHMENT A - FAMILY RESOURCE CENTER SERVICES

1.	POPULATION TO BE SERVED.....	1
2.	DEFINITIONS.....	1
3.	OUTCOME OBJECTIVES.....	4
4.	DESIGNATED LEAD AGENCY	5
5.	HOURS OF OPERATION.....	7
6.	FRC GENERAL REQUIREMENTS AND CHARACTERISTICS.....	8
7.	FRC SERVICE REQUIREMENTS.....	10
8.	ADDITIONAL CONTRACTOR RESPONSIBILITIES	21
9.	FACILITIES	23

10. REPORTING REQUIREMENTS..... 24

11. MEETINGS..... 25

12. UTILIZATION REVIEW 25

13. BUDGET..... 26

14. STAFFING REQUIREMENTS..... 28

15. TRAINING 35

16. DATA ENTRY AND DATA SUBMISSION REQUIREMENTS..... 36

17. SUSTAINABILITY 37

18. QUALITY ASSURANCE/QUALITY CONTROL..... 38

ATTACHMENT B - COUNTY OF ORANGE INFORMATION TECHNOLOGY SECURITY PROVISIONS

ATTACHMENT C - STATE PRIVACY AND SECURITY PROVISIONS

ATTACHMENT D - COUNTY OF ORANGE INFORMATION TECHNOLOGY SECURITY GUIDELINES

1. TERM

The term of this Contract shall commence on July 1, 2025, and terminate on June 30, 2028, unless earlier terminated pursuant to the provisions of Paragraph 41 of this Contract; 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. This Contract may be renewed thereafter for a two-year term upon mutual agreement of both parties. The COUNTY does not have to provide a reason if it elects not to renew this Contract.

2. ALTERATION OF TERMS

2.1 This Contract, including any Attachment(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 Contract. No addition to, or alteration of, the terms of this Contract, whether written or verbal, are valid or binding unless made in the form of a written amendment to this Contract which is formally approved and executed by both parties.

2.2 The various headings, numbers, and organization herein are for the purpose of convenience only and shall not limit or otherwise affect the Contract.

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 Contract. 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, and employees 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

- 4.1 CONTRACTOR agrees to provide those services, facilities, equipment, and supplies, for the Provision of Family Resource Center Services, as described in Attachment A. CONTRACTOR shall operate continuously throughout the term of this Contract 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 funding obligation, as set forth in this Contract, 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 and its personnel, described in Paragraph 26 of this Contract, who are subject to individual registration and/or licensing requirements, have all necessary licenses and permits required by the laws of the United States, State of California (hereinafter referred to as "State"), County of Orange, and all other appropriate governmental agencies to perform the services described in this Contract, and agrees to maintain, and require its personnel to maintain, these licenses and permits in effect for the duration of this Contract. 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. CONTRACTOR must notify ADMINISTRATOR within one (1) business day of any change in license or permit status (e.g., becoming expired,

inactive, etc.).

- 5.2 In the performance of this Contract, 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; and all applicable laws and regulations of the United States, State of California, County of Orange, and 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.
- 5.3 For federally funded Contracts 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.
- 5.4 CONTRACTOR shall cooperate with the California Department of Social Services (CDSS) on the implementation, monitoring, and evaluation of the State's Child Abuse and Neglect Prevention and Intervention Program, and shall comply, to the mutual satisfaction of COUNTY and CDSS, with any and all reporting and evaluation requirements established by CDSS.

6. DELEGATION AND ASSIGNMENT/CHANGE OF OWNERSHIP

6.1 Delegation and Assignment

- 6.1.1 In the performance of this Contract, 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 Contract requiring COUNTY approval.
- 6.1.2 COUNTY reserves the right to immediately terminate the Contract in the

event COUNTY determines that the assignee is not qualified or otherwise acceptable to COUNTY for the provision of services under the Contract.

6.2 Change of Ownership

CONTRACTOR agrees that if there is a change or transfer in ownership of CONTRACTOR's business prior to completion of this Contract, and COUNTY agrees to an assignment of the Contract, the new owners shall be required, under the terms of sale or other instruments of transfer, to assume CONTRACTOR's duties and obligations contained in this Contract and complete them to the satisfaction of COUNTY.

7. SUBCONTRACTS

7.1 CONTRACTOR shall not subcontract for services under this Contract 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.

7.1.1 Subcontracts of \$50,000 or less

7.1.1.1 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 fifty thousand dollars (\$50,000) or less during the term of this Contract. 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.

7.1.2 Subcontracts in excess of \$50,000

7.1.2.1 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 fifty thousand dollars (\$50,000) during the term of this Contract. 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.

7.1.2.2 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 fifty thousand dollars (\$50,000) during the term of this Contract. 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 fifty thousand dollars (\$50,000) during the term of this Contract.

7.1.2.3 CONTRACTOR and its subcontractor(s) shall establish and maintain accurate and complete financial records related to services provided under the terms of this Contract. 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.

8. FORM OF BUSINESS ORGANIZATION/NAME CHANGE

8.1 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:

- 8.1.1 The form of CONTRACTOR's business organization, i.e., proprietorship, partnership, corporation, etc.
- 8.1.2 A detailed statement indicating the relationship of CONTRACTOR, by way of ownership or otherwise, to any parent organization or individual.
- 8.1.3 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 Contract.

8.2 Change in Form of Business Organization

If, during the term of this Contract, the form of CONTRACTOR's business organization changes, or the ownership of CONTRACTOR changes, or when changes occur between CONTRACTOR and other businesses that could impact services provided through this Contract, 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 Contract.

8.3 Name Change

CONTRACTOR must notify COUNTY, in writing, of any change in CONTRACTOR's status with respect to name changes that do not require an assignment of the Contract. While CONTRACTOR is required to provide name change information without prompting from the COUNTY, CONTRACTOR must also provide an update to COUNTY of its status upon request by COUNTY.

9. NON-DISCRIMINATION

- 9.1 In the performance of this Contract, 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.

9.2 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 9 et seq.

9.3 Non-Discrimination in Employment

9.3.1 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).

9.3.2 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.

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

California Department of Fair Employment

2218 Kausen Drive, Suite 100
Elk Grove, CA 95758
Telephone: (800) 884-1684
(800) 700-2320 (TTY)

9.4 Non-Discrimination in Service Delivery

- 9.4.1 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 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 9.4 et seq.
- 9.4.2 CONTRACTOR shall provide any and all clients desirous of filing a formal complaint any and all information as appropriate:

9.4.2.1 Pamphlet: “Your Rights Under California Welfare Programs”
(PUB 13)

9.4.2.2 Discrimination Complaint Form

9.4.2.3 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 8-16-70

Sacramento, CA 94244-2430

Telephone: (916) 654-2107

Toll Free: (866) 741-6241

Federal Civil Rights Contact:

Office for Civil Rights

U.S. Department of Health and Human Services

90 7th Street, Suite 4-100

San Francisco, CA 94103

Customer Response Center: (800) 368-1019

9.4.3 The following websites provide Civil Rights information, publications and/or forms:

9.4.3.1 <https://www.cdss.ca.gov/Portals/9/FMUForms/M-P/PUB470.pdf?ver=2021-05-10-164956-817> (Pub 470 - Your rights Under Adult Protective Services)

9.4.3.2 <http://www.cdss.ca.gov/inforesources/Civil-Rights/Your-Rights-Under-California-Welfare-Program> (Pub 13 - Your

Rights Under California Welfare Programs)

9.4.3.3 <http://ssa.ocgov.com/about/services/contact/complaints/comply>

[Social Services Agency (SSA) Contractor and Vendor Compliance page]

10. NOTICES

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

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

CONTRACTOR: All For Kids Organization
1910 Magnolia Ave.
Los Angeles, CA 90007

10.2 All notices shall be deemed effective when in writing and when:

- 10.2.1 Deposited in the United States mail, first class postage prepaid and addressed as shown in Subparagraph 10.1 above;
- 10.2.2 Sent by Email;
- 10.2.3 Faxed and transmission confirmed; or
- 10.2.4 Accepted by U.S. Postal Services Express Mail, Federal Express, United Parcel Service, or any other expedited delivery service.

10.3 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.

11. NOTICE OF DELAYS

Except as otherwise provided under this Contract, when either party has knowledge that any actual or potential situation is delaying or threatens to delay the timely

performance of this Contract, that party shall, within one (1) business day, give notice thereof, including all relevant information with respect thereto, to the other party.

12. INDEMNIFICATION

12.1 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 Contract. 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.

13. INSURANCE

13.1 Prior to the provision of services under this Contract, CONTRACTOR agrees to carry all required insurance at CONTRACTOR's expense, including all endorsements required herein, necessary to satisfy COUNTY that the insurance provisions of this Contract have been complied with. CONTRACTOR agrees to keep such insurance coverage current, provide Certificates of Insurance and endorsements to ADMINISTRATOR during the entire term of this Contract.

13.2 CONTRACTOR shall ensure that all subcontractors performing work on behalf of CONTRACTOR pursuant to this Contract 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

Contract. 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 Contract for inspection by COUNTY representative(s) at any reasonable time.

13.3 All self-insured retentions (SIRs) shall be clearly stated on the Certificate of Insurance. Any SIRs in excess of fifty thousand dollars (\$50,000) shall specifically be approved by the COUNTY's Risk Manager, or designee. COUNTY reserves the right to require current audited financial reports from CONTRACTOR. If CONTRACTOR is self-insured, CONTRACTOR will indemnify COUNTY for any and all claims resulting or arising from CONTRACTOR's services in accordance with the indemnity provision stated in this Contract.

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

13.5 Qualified Insurer

13.5.1 The policy or policies of insurance 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).

13.5.2 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 ratings.

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

<u>Coverage</u>	<u>Minimum Limits</u>
Commercial General Liability	\$1,000,000 per occurrence \$2,000,000 aggregate

Automobile Liability including coverage for owned or scheduled, non-owned, and hired vehicles	\$1,000,000 combined single limit each accident
-----------------------------------------------------------------------------------------------	-------------------------------------------------

Workers' Compensation

Statutory

Employer's Liability Insurance	\$1,000,000 per accident or disease
--------------------------------	-------------------------------------

Network Security & Privacy Liability	\$1,000,000 per claims-made
--------------------------------------	-----------------------------

Professional Liability Insurance	\$1,000,000 per claims-made or occurrence
	\$1,000,000 aggregate

Sexual Misconduct Liability	\$1,000,000 per occurrence
-----------------------------	----------------------------

13.5.4 Increased insurance limits may be satisfied with Excess/Umbrella policies. Excess/Umbrella policies when required must provide Follow Form coverage.

13.6 Required Coverage Forms

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

13.6.2 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.

13.7 Required Endorsements

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

13.7.1.1 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, employees, and agents as Additional Insureds or provide blanket coverage, which will state AS REQUIRED BY WRITTEN CONTRACT.

13.7.1.2 A primary non-contributory 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 shall be excess and non-contributory.

13.7.2 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, employees, and agents or provide blanket coverage, which will state AS REQUIRED BY WRITTEN CONTRACT.

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

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

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

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

13.9 CONTRACTOR shall provide thirty (30) days prior written notice to the County of any policy cancellation or non-renewal and ten (10) days prior written notice where cancellation is due to 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 Contract.

13.10 If CONTRACTOR's Professional Liability and/or Network Security & Privacy Liability policy are a "Claims-Made" policy(ies), CONTRACTOR shall agree to the following:

13.10.1 The retroactive date must be shown and must be before the date of the Contract or the beginning of the Contract services.

13.10.2 Insurance must be maintained, and evidence of insurance must be provided for at least three (3) years after expiration or earlier termination of Contract services.

13.10.3 If coverage is canceled or non-renewed, and not replaced with another claims-made policy form with a retroactive date prior to the effective date of the Contract services, Contractor must purchase an extended reporting period for a minimum of three (3) years after expiration of earlier termination of the Contract.

13.11 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).

13.12 Insurance certificates should be forwarded to COUNTY at the address indicated in Paragraph 10 of this Contract.

13.13 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.

13.14 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 Contract. Any increase or decrease in insurance will be as deemed by County of

Orange Risk Manager as appropriate to adequately protect COUNTY.

13.15 COUNTY shall notify CONTRACTOR in writing of changes in the insurance requirements. If CONTRACTOR does not provide acceptable Certificates of Insurance and endorsements to COUNTY incorporating such changes within thirty (30) days of receipt of such notice, this Contract may be in breach without further notice to CONTRACTOR, and COUNTY shall be entitled to all legal remedies.

13.16 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 Contract, nor act in any way to reduce the policy coverage and limits available from the insurer.

14. NOTIFICATION OF LITIGATION, INCIDENTS, CLAIMS, OR SUITS

CONTRACTOR shall report to COUNTY, in writing within twenty-four (24) hours of occurrence, the following:

14.1 Any instance in which CONTRACTOR becomes a party to any litigation against COUNTY, or a party to litigation that may reasonably affect CONTRACTOR's performance under this Contract. While CONTRACTOR is required to provide this information without prompting from COUNTY, any time there is a change to CONTRACTOR's litigation status, CONTRACTOR must also provide an update to COUNTY whenever requested by COUNTY.

14.2 Any accident or incident relating to services performed under this Contract that involves injury or property damage which may result in the filing of a claim or lawsuit against CONTRACTOR and/or COUNTY.

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

14.4 Any injury to an employee of CONTRACTOR that occurs on COUNTY property.

14.5 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 Contract.

- 14.6 Any Notice of Contract Breach, or equivalent, received from any entity for whom CONTRACTOR is providing the same or similar services, under a written contract, regardless of service location or jurisdiction.

15. CONFLICT OF INTEREST

- 15.1 CONTRACTOR shall exercise reasonable care and diligence to prevent any actions or conditions that could result in a conflict with COUNTY interests. In addition to the CONTRACTOR, this obligation shall apply to, CONTRACTOR's employees, agents, and subcontractors associated with the provision of goods and services provided under this Contract. The CONTRACTOR's efforts shall include, but not be limited to, establishing rules and procedures preventing its employees, agents, and subcontractors from providing or offering gifts, entertainment, payments, loans, or other considerations which could be deemed to influence or appear to influence COUNTY staff or elected officers in the performance of their duties.

- 15.2 CONTRACTOR shall notify COUNTY, in writing, of any potential conflicts of interest between CONTRACTOR and COUNTY that may arise prior to, or during the period of, Contract performance. While CONTRACTOR will be required to provide this information without prompting from COUNTY any time there is a change regarding conflict of interest, CONTRACTOR must also provide an update to COUNTY whenever requested by COUNTY.

16. 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.

17. SUPPLANTING GOVERNMENT FUNDS

CONTRACTOR shall not supplant any federal, State, or COUNTY funds intended for the purposes of this Contract with any funds made available under this Contract. 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 Contract, 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.

18. EQUIPMENT

18.1 All items purchased with funds provided under this Contract, 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 Contract. Upon the termination of this Contract, 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:

- 18.1.1 To maintain all items of Capital Equipment in good working order and condition, normal wear and tear excepted.
- 18.1.2 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.
- 18.1.3 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.
- 18.1.4 To purchase a policy or policies of insurance covering loss or damage to any and all Capital Equipment purchased under this Contract, 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.

18.2 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 Contract which are appropriate and directly related to CONTRACTOR's service or activity under the terms of this Contract. 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.

18.3 Computer Equipment

No computers and/or personal electronic devices, such as tablets and laptop computers, or any component thereof, may be purchased with funds provided under this Contract, 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 above in Subparagraphs 18.1.1 to 18.1.4, and, at the sole discretion of ADMINISTRATOR, become the property of COUNTY upon termination of this Contract.

19. BREACH SANCTIONS

19.1 Failure by CONTRACTOR to comply with any of the provisions, covenants, or conditions of this Contract shall be a material breach of this Contract. 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 Contract:

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

19.1.2 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

19.1.3 Offset against any monies billed by CONTRACTOR but yet unpaid by COUNTY those monies disallowed pursuant to Subparagraph 19.1.2 above.

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

20. PAYMENTS

20.1 Maximum Contractual Funding Obligation

The maximum funding obligation of COUNTY under this Contract shall not exceed the amount of \$18,000,000, or actual allowable costs, whichever is less. The estimated annual amount for each twelve (12) month period is as follows:

\$6,000,000 for July 1, 2025, through June 30, 2026;

\$6,000,000 for July 1, 2026, through June 30, 2027; and

\$6,000,000 for July 1, 2027, through June 30, 2028.

20.2 Allowable Costs

During the term of this Contract, COUNTY shall pay CONTRACTOR monthly in arrears, for actual allowable costs incurred and paid by CONTRACTOR pursuant to this Contract, as defined in Title 2 CFR Part 200, or as approved by ADMINISTRATOR. However, COUNTY, at its sole discretion, may pay CONTRACTOR for anticipated allowable costs that will be incurred by CONTRACTOR for the month of June during the term of the contract, during the month of such anticipated expenditure.

20.3 Claims

20.3.1 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, except as detailed below in Subparagraph 20.3.4. 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 Jr. Day, President Lincoln's Birthday, Presidents' Day, Memorial Day, Independence Day, Labor Day, Native American Day, Veterans Day, Thanksgiving Day, Friday after Thanksgiving Day, and Christmas Day.

20.3.2 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 25 of this Contract.

20.3.3 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.

20.3.4 Year-End and Final Claims

20.3.4.1 CONTRACTOR shall submit a final claim for each COUNTY fiscal year, July 1 through June 30, covered under the term of this Contract, as stated in Paragraph 1, by no later than August 30th of each corresponding COUNTY fiscal year. Claims received after August 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.

20.3.4.2 The basis for final settlement shall be the actual allowable costs as defined in Title 45 CFR and 2 CFR, Part 200, incurred and paid by CONTRACTOR pursuant to this Contract; limited, however, to the maximum funding 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.

21. OVERPAYMENTS

Any payment(s) made by COUNTY to CONTRACTOR in excess of that to which CONTRACTOR is entitled under this Contract shall be repaid to COUNTY, in accordance with any applicable regulations and/or policies in effect during the term of this Contract, 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.

22. OUTSTANDING DEBT

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

23. FINAL REPORT

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

24. INDEPENDENT AUDIT

24.1 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 Contract in compliance with 31 USC 7501 – 7507, as well as its implementing regulations under 2 CFR Part 200, Uniform Administrative Requirements, Cost Principles and Audit Requirements for Federal Awards. If CONTRACTOR is not subject to the aforementioned regulations for any year covered during the term of this Contract, CONTRACTOR shall provide ADMINISTRATOR an Independent Auditor's Report of CONTRACTOR's financial statements. The audit must be performed in accordance with generally accepted government auditing standards. 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.

24.2 It is mutually understood that CONTRACTOR's yearly fiscal cycle covers July 1 through June 30. CONTRACTOR shall provide ADMINISTRATOR copies of organization-wide audits for each of the fiscal cycles corresponding with the term of this Contract. 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 Contract 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.

25. RECORDS, INSPECTIONS, AND AUDITS

25.1 Financial Records

25.1.1 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 Contract, or until all pending COUNTY, State, and federal audits are completed, whichever is later.

25.1.2 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.

25.2 Client Records

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

25.2.2 CONTRACTOR shall keep all COUNTY data provided to CONTRACTOR during the term(s) of this Contract for a minimum of five (5) years from the date of final payment under this Contract, 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 Contract, CONTRACTOR shall relinquish control with respect to COUNTY data to COUNTY in accordance with Subparagraph 41.2 of this contract.

25.2.3 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 Contract.

25.3 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 Contract, may be subject to public disclosure. COUNTY will not be liable for any such disclosure.

25.4 Inspections and Audits

- 25.4.1 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 Contract. 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 Contract and the premises in which it is being performed.
- 25.4.2 CONTRACTOR shall make its books and records available within the borders of Orange County within ten (10) days of receipt of written demand by ADMINISTRATOR.
- 25.4.3 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 records.
- 25.4.4 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 Contract.

25.5 Evaluation Studies

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.

26. PERSONNEL DISCLOSURE

- 26.1 This Paragraph 26 applies to all of CONTRACTOR's personnel providing services through this Contract, paid and unpaid, including those identified in Paragraph 14 of Attachment A (hereinafter referred to as "Personnel").
- 26.2 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:
- 26.2.1 Names and dates of birth of all Personnel by title, whose direct services are required to provide the programs described herein;
 - 26.2.2 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;
 - 26.2.3 The professional degree, if applicable, and experience required for each position; and
 - 26.2.4 The language skill, if applicable, for all Personnel.
- 26.3 Where authorized by law, and in a manner consistent with California Government Code Section 12952, CONTRACTOR shall require prospective Personnel to provide detailed information regarding the conviction of a crime, by any court, for offenses other than minor traffic offenses. Information discovered subsequent to the hiring or promotion of any prospective Personnel shall be cause for termination from the performance of services under this Contract.
- 26.4 Where authorized by law, CONTRACTOR shall conduct, at no cost to COUNTY, a clearance on the following public websites of the names and dates of birth for all Personnel who will have direct, interactive contact with clients served through this Contract: U.S. Department of Justice National Sex Offender Website (www.nsopw.gov) and Megan's Law Sex Offender Registry (www.meganslaw.ca.gov).
- 26.5 Where authorized by law, CONTRACTOR shall conduct, at no cost to COUNTY, a criminal record background check on all Personnel who will have direct,

interactive contact with clients served through this Contract. 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 Contract.

- 26.6 CONTRACTOR shall ensure that clearances and background checks described above in Subparagraphs 26.4 and 26.5 are completed prior to CONTRACTOR's Personnel providing services under this Contract.
- 26.7 In the event a record is revealed through the processes described in above Subparagraphs 26.4 and 26.5, COUNTY will be available to consult with CONTRACTOR on appropriateness of Personnel providing services through this Contract.
- 26.8 CONTRACTOR warrants that all Personnel assigned by CONTRACTOR to provide services under this Contract 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 Contract. CONTRACTOR shall maintain records of background investigations and reference checks undertaken and coordinated by CONTRACTOR for Personnel assigned to provide services under this Contract, for a minimum of five (5) years from the date of final payment under this Contract, or until all pending COUNTY, State, and federal audits are completed, whichever is later, in compliance with all applicable laws.
- 26.9 CONTRACTOR shall immediately notify ADMINISTRATOR concerning the arrest and/or subsequent conviction, for offenses, other than minor traffic offenses, of any Personnel performing services under this Contract, when such information becomes known to CONTRACTOR. ADMINISTRATOR may determine whether such Personnel may continue to provide services under this Contract 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 Contract, pursuant to Paragraph 19 above.

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

26.11 COUNTY shall have the right to require CONTRACTOR to remove any Personnel from the performance of services under this Contract. At the request of COUNTY, CONTRACTOR shall immediately replace said Personnel.

26.12 CONTRACTOR shall notify COUNTY immediately when Personnel is terminated for cause from working on this Contract.

26.13 Disqualification, if any, of CONTRACTOR Personnel, pursuant to this Paragraph 26 shall not relieve CONTRACTOR of its obligation to complete all work in accordance with the terms and conditions of this Contract.

27. 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 Contract 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, and 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 Contract.

28. CHILD AND DEPENDENT ADULT/ELDER ABUSE REPORTING

CONTRACTOR shall establish a procedure acceptable to ADMINISTRATOR to ensure that all employees, agents, subcontractors, and all other individuals performing services under this Contract 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 employees, agents, subcontractors, and all other individuals performing services under this Contract 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 shall 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, agents, subcontractors, and all other individuals performing services under this Contract. CONTRACTOR shall require all of its employees, agents, subcontractors, and all other individuals performing services under this Contract to sign an agreement with CONTRACTOR before commencing the provision of any such services, agreeing to maintain confidentiality pursuant to State and federal law and the terms of this

Contract.

30.3 CONTRACTOR shall inform all of its employees, agents, subcontractors, and all other individuals performing services under this Contract 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 Contract.

30.5 CONTRACTOR agrees to maintain the confidentiality of its records with respect to Juvenile Court matters, in accordance with WIC Section 827, all applicable statutes, caselaw, and Orange County Juvenile Court Policy regarding Confidentiality, as it now exists or may hereafter be amended.

30.5.1 No access, disclosure, or release of information regarding a child who is the subject of Juvenile Court proceedings shall be permitted except as authorized. If authorization is in doubt, no such information shall be released without the written approval of a Judge of the Juvenile Court.

30.5.2 CONTRACTOR must receive prior written approval of the Juvenile Court before allowing any child to be interviewed, photographed, or recorded by any publication or organization, or to appear on any radio, television, or internet broadcast or make any other public appearance. Such approval shall be requested through child's Social Worker.

31. SECURITY

31.1 CONTRACTOR shall abide by the requirements in Attachment B, C, and D.

32. 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 Contract, including those covered by copyright.

33. 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 Contract 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.

34. SERVICES DURING EMERGENCY AND/OR DISASTER

34.1 CONTRACTOR acknowledges that service usage may surge during or after an emergency or disaster. For purposes of this Contract, an emergency is defined as a sudden, urgent, usually unexpected occurrence or event requiring immediate action to protect the health and well-being of COUNTY residents. A disaster is defined as an occurrence that has resulted in property damage, deaths, and/or injuries to a community. Emergencies and/or disasters as described above may require resources or support beyond the local government's capability and will typically involve a proclamation of a local emergency by the local governing body (e.g., city council, county board of supervisors, or state) and may be declared at the federal level by the President of the United States.

34.2 CONTRACTOR agrees to collaborate with COUNTY, on an urgent basis, to adjust service delivery in a manner that assists COUNTY in meeting the needs of clients COUNTY identifies as being impacted by emergencies and/or disasters. Time limited adjustments may include, but are not limited to: providing services at different location(s), assigning staff to work days or hours beyond typical work schedules or that may exceed contracted Full Time Equivalents (FTEs), reassigning staff to an assignment in which their experience or skill is needed, and prioritizing services for staff as requested by COUNTY.

34.3 CONTRACTOR shall service COUNTY during emergencies and/or declared disaster under the same terms and conditions that apply during non-emergency/disaster conditions. With the exception of overtime hours which require pre-authorization, reimbursement of ordinary expenditures provided during or after

an emergency/disaster shall be calculated by the same rates that apply during non-emergency/disaster conditions. Additionally, any costs to continue services to clients during an emergency and/or disaster shall be incurred by the Contractor. These costs may include, but are not limited to: Personal Protective Equipment or other supplies necessary to conduct business during an emergency and/or disaster.

- 34.4 Emergency Publicity & Outreach: In response to natural disasters and local emergencies, at the direction of the COUNTY, CONTRACTOR shall assist the COUNTY with publicity of COUNTY provided emergency benefits informational materials and messaging, to provide CONTRACTOR's clientele with helpful emergency benefits and resource information during emergencies.

35. PUBLICITY, LITERATURE, ADVERTISEMENTS AND SOCIAL MEDIA

- 35.1 COUNTY owns all rights to the name, logos, and symbols of COUNTY. The use and/or reproduction of COUNTY's name, logos, or symbols for any purpose, including commercial advertisement, promotional purposes, announcements, displays, or press releases, without COUNTY's prior written consent is expressly prohibited.
- 35.2 CONTRACTOR may develop and publish information related to this Contract where all of the following conditions are satisfied:
- 35.2.1 ADMINISTRATOR provides its written approval of the content and publication of the information at least thirty (30) days prior to CONTRACTOR publishing the information, unless a different timeframe for approval is agreed upon by the ADMINISTRATOR;
 - 35.2.2 Unless directed otherwise by ADMINISTRATOR, the information includes a statement that the program, wholly or in part, is funded through County, State, and Federal Government funds.
 - 35.2.3 The information does not give the appearance that the COUNTY, its officers, employees, or agencies endorse:
 - 35.2.3.1 Any commercial product or service; and
 - 35.2.3.2 Any product or service provided by CONTRACTOR, unless

approved in writing by ADMINISTRATOR; and

35.2.4 If CONTRACTOR uses social media (such as Facebook, Twitter, YouTube, or other publicly available social media sites) to publish information related to this Contract, CONTRACTOR shall develop social media policies and procedures and have them available to the ADMINISTRATOR. 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 Contract. The policy is available on the Internet at <https://cio.ocgov.com/egovernment-policies>.

36. REPORTS

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

36.2 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 Contract, 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.

37. 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).

38. 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:

- 38.1 No facility to be utilized in the performance of the proposed grant has been listed on the EPA List of Violating Facilities;
- 38.2 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
- 38.3 It will notify COUNTY and EPA about any known violation of the above laws and regulations.

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

39.1 CONTRACTOR shall be in compliance with Section 319 of Public Law 101-121 pursuant to Section 1352, Title 31, U.S. Code. 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 includes the text below in Subparagraphs 39.1.1.1 - 39.1.1.4.

39.1.1 The undersigned certifies to the best of his or her knowledge and belief that:

39.1.1.1 No federal appropriated funds have been paid or will be paid, by or on behalf of the undersigned, to any person for influencing or attempting to influence an officer or employee of an agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with the awarding of any federal contract, the making of any federal grant, the making of any federal loan, the entering into of any cooperative contract, and the extension, continuation, renewal, amendment, or modification of any federal contract, grant, loan or cooperative contract.

39.1.1.2 If any funds other than federal appropriated funds have been paid

or will be paid to any person for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with this Contract, grant, loan, or cooperative contract, the undersigned shall complete and submit Standard Form-LLL "Disclosure Form to Report Lobbying," in accordance with its instructions.

39.1.1.3 The undersigned shall require that the language of this certification be included in the award documents for all subawards at all tiers (including subcontracts, subgrants, and contracts under grants loans and cooperative contracts) and that subrecipients shall certify and disclose accordingly.

39.1.1.4 This certification is a material representation of fact upon which reliance was placed when this transaction was made or entered into. Submission of this certification is a prerequisite for making or entering into this transaction imposed by Section 1352, Title 31 U.S. Code. Any person who fails to file the required certification shall be subject to a civil penalty of not less than \$10,000 and not more than \$100,000 for each such failure.

40. POLITICAL ACTIVITY

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

41. TERMINATION PROVISIONS

41.1 ADMINISTRATOR may terminate this Contract 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 Contract 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 Contract shall relieve COUNTY of all further obligations under this Contract.

- 41.2 For ninety (90) calendar days prior to the expiration date of this Contract, or upon notice of termination of this Contract (“Transition Period”), CONTRACTOR agrees to cooperate with ADMINISTRATOR in the orderly transfer of service responsibilities, 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.
- 41.3 In the event of termination of this Contract, 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 Contract.
- 41.4 The obligations of COUNTY under this Contract 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 Contract remains in effect or operation. In the event that such funding is terminated or reduced, ADMINISTRATOR may immediately terminate this Contract, reduce COUNTY’s maximum funding obligation, or modify this Contract, without penalty. The decision of ADMINISTRATOR shall be binding on CONTRACTOR. ADMINISTRATOR will provide CONTRACTOR with written notification of such determination. CONTRACTOR shall immediately

comply with ADMINISTRATOR's decision.

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

42. COOPERATIVE CONTRACT

- 42.1 This Contract is a cooperative contract and may be utilized by all County of Orange departments.

- 42.2 The provisions and pricing of this Contract may be extended, at the option of Contractor, to any Municipal, County, Public Utility, Hospital, Educational Institution, or any other non-profit or governmental organization (the "Cooperative Program"). Parties in a Cooperative Program wishing to use this Contract will be responsible for issuing their own purchase documents / price agreements, providing for their own acceptance, and making any subsequent payments. Contractor shall be required to include in any agreement entered into with another agency or entity that is entered into pursuant to the provisions and pricing of this Contract a clause that binds the parties to the agreement to "indemnify, defend with counsel approved in writing by the County of Orange, California ("County"), and hold County, its 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" under the agreement. Failure to so include this clause voids the Contract's extension to a Cooperative Program and will be considered a material breach of this Contract and grounds for immediate Contract termination. The cooperative entities are responsible for obtaining all certificates of insurance and bonds required. The County of Orange makes no guarantee of usage by other users of this Contract.

- 42.3 Subordinate contracts must be executed prior to the expiration or earlier termination

of this Contract and may survive the expiration of this Contract. This Cooperative Contract provision shall survive expiration or termination of this Contract.

43. GOVERNING LAW AND VENUE

This Contract 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 Contract, 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

- 44.1 The parties agree that separate copies of this Contract may be signed by each of the parties, and this Contract will have the same force and effect as if the original had been signed by all the parties.
- 44.2 CONTRACTOR represents and warrants that the person executing this Contract 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 Contract and that all requirements of CONTRACTOR have been fulfilled to provide such actual authority.

IN WITNESS WHEREOF, the Parties hereto have executed this Contract the date set forth opposite their signatures. If Contractor is a corporation, Contractor shall provide two (2) signatures as follows: 1) the first signature must be either the Chairman of the Board, the President, or any Vice President; 2) the second signature must be that of the Secretary, an Assistant Secretary, the Chief Financial Officer, or any Assistant Treasurer. In the alternative, a single corporate signature is acceptable when accompanied by a corporate resolution or by-laws demonstrating the legal authority of the signature to bind the company.

Contractor: ALL FOR KIDS ORGANIZATION

Ron Brown

President & CEO

Print Name

Title

Signed by:

Ron Brown

4/9/2025 | 12:39:43 PM PDT

03B4BA0EED594E9...

Signature

Date

Print Name

Title

Signature

Date

Contractor: OLIVE CREST

Donald verleur

CEO

Print Name

Title

Signed by:

Donald Verleur

4/11/2025 | 3:35:36 PM PDT

CD27A64C1CE54F0...

Signature

Date

Print Name

Title

Signature

Date

Contractor: HUMAN OPTIONS, INC.

Sara Behmerwohld

Chief Operations Officer

Print Name

Title

DocuSigned by:
Sara Behmerwohld
8BA8BAEDAAA04BB...
Signature

4/9/2025 | 12:08:33 PM PDT

Date

Print Name

Title

Signature

Date

County of Orange, a political subdivision of the State of California

Deputized Designee Signature:

Print Name

Deputy Purchasing Agent
Title

Signature

Date

APPROVED AS TO FORM
COUNTY COUNSEL
COUNTY OF ORANGE, CALIFORNIA

Carolyn Frost

Deputy County Counsel

Print Name
DocuSigned by:
Carolyn S. Frost
D3AB98D76D0B425...
Signature

Title

4/14/2025 | 9:31:18 AM PDT

Date

ATTACHMENT A
SCOPE OF WORK

FOR THE PROVISION OF
FAMILY RESOURCE CENTER SERVICES

1. POPULATION TO BE SERVED

1.1 CONTRACTOR shall provide services to families referred by the Social Services Agency (SSA). CONTRACTOR shall provide Family Resource Center (FRC) services, as described in Paragraph 7 of this Attachment A, with a preventative and early intervention approach, to: birth, kinship, blended, adoptive, and Resource Families with children, ages birth to their eighteenth birthday (0-18), who are at risk of or are experiencing child abuse and neglect; families who are living in poverty or suffering economic hardship, domestic violence, unemployment, substance use disorder, teen pregnancy, and unhealthy parenting; families involved with and/or receiving child welfare services; non-minor dependents ages eighteen (18) to twenty-one (21) years old, who are being served by child welfare or probation agencies and who are under the jurisdiction of the Orange County Juvenile Court; trafficked children and youth; Lesbian, Gay, Bisexual, Transgender, and Queer (LGBTQ) Youth; homeless families, unaccompanied youth, and those families at-risk of homelessness; military families; families with persons with disabilities; and families who are receiving public assistance benefits including, but not limited to, California Work Opportunity and Responsibility (CalWORKs), CalFresh, and/or Medi-Cal from SSA. The population to be served as defined in this Paragraph shall hereinafter be referred to as “PARTICIPANTS” or “FAMILIES.”

1.2 CONTRACTOR shall provide FRC services primarily to those PARTICIPANTS residing in the surrounding communities.

2. DEFINITIONS

2.1 California Evidence-Based Clearinghouse for Child Welfare: An online resource for child welfare professionals, and others who are committed to improving

outcomes for children and families and includes a database of programs, practices, and interventions related to child welfare and family well-being.

- 2.2 CalWORKs: California Work Opportunity and Responsibility to Kids Act of 1997 as described in California WIC Section 11200 et seq. CalWORKs is a program administered by County Welfare Departments and provides cash assistance, case management, job services, job training, and supportive services to assist CalWORKs recipients in overcoming barriers to obtaining and/or maintaining stable employment, with the goal of achieving economic self-sufficiency.
- 2.3 CalFresh: CalFresh provides monthly food benefits to individuals and families with low-income and provides economic benefits to communities.
- 2.4 Case Management Team (CMT) Meetings: A collaboration among Contractor Partner Agencies by meeting on a weekly basis to effectively coordinate PARTICIPANT services. A CMT is comprised of a Multidisciplinary Personnel Team as defined in Subparagraph 2.14 of Attachment A.
- 2.5 Children and Family Services (CFS): The division in SSA that provides services to protect children from abuse and neglect, and at-risk Families.
- 2.6 Community Engagement Advisory Council (CEAC): A partnership of multiple agencies and community members that strive to achieve positive outcomes for the populations they serve and build an interdependent system to address issues and opportunities.
- 2.7 Collaborative: A partnership of multiple agencies that strive to achieve positive outcomes for the populations they serve and build an interdependent system to address issues and opportunities. Collaboratives also share resources and responsibilities to jointly plan, implement, and evaluate programs to achieve common goals.
- 2.8 Contracted Partner Agency: A funded or non-funded partner agency in partnership with the County that provides contracted FaCT FRC core services through a

collaborative FRC agreement or an individual agency agreement.

- 2.9 Culturally Responsive: To possess a general knowledge of cultural values and mores of individuals from diverse ethnic groups; the ability to recognize, respect, affirm, and value the worth of individuals from diverse ethnic groups; and the ability to interact responsively, respectfully, and effectively with people from diverse cultures, classes, races, ethnic groups, and religious backgrounds in a manner that recognizes, affirms, and values the worth of individuals, families, and communities, as well as protecting the dignity of each person.
- 2.10 Differential Response - Path Two (DR - Path Two): A concept that child safety is a responsibility shared by the family, community, and child welfare agencies. DR's primary goal is to engage a greater number of families in services within the community without bringing them into the child welfare system and reduce the recurrence of child maltreatment. DR services are indicated when reported allegations meet statutory definitions of abuse or neglect, yet an initial assessment made by SSA CFS determines that with targeted services, a family is likely to make needed changes to improve child safety.
- 2.11 Families and Communities Together (FaCT) Platform: A public-private partnership that supports FRCs and provides program development and administration, funding, and training. FaCT receives federal, State, and County funding, as well as volunteer, in-kind support, and private donations.
- 2.12 LGBTQ Youth: Acronym stands for Lesbian, Gay, Bisexual, Transsexual, and Questioning and is used by youth who are not heterosexual and/or identify with the sex they were not assigned at birth.
- 2.13 Military Families: A family unit consisting of active service members, reservists, veterans (regardless of discharge status), and their children, spouses, partners, and loved ones.
- 2.14 Multidisciplinary Personnel Team (MDT): Pursuant to WIC Section 15610.55 (a), a team of two (2) or more persons trained in the prevention, identification, and

treatment of child abuse and neglect cases and who are qualified to provide a broad range of services related to child abuse. The team may include, but not be limited to, trained counseling personnel, police officers or other law enforcement agents, medical personnel, social workers, public or private school teachers, administrative officers, supervisors of child welfare, or certified pupil personnel employees. The MDT meets regularly to discuss children and families of alleged child abuse reports that do not meet the statutory definition of child abuse or neglect but may result in the neglect, abuse, exploitation, or delinquency of children, and which could be addressed by the MDT and prevent the unnecessary separation of families.

- 2.15 Non-Minor Dependent (NMD): Pursuant to WIC Section 11400(v), a foster youth who has attained the age of eighteen (18) years while in foster care and has an open case with the Juvenile Court who may remain under the jurisdiction of Juvenile Court, up to twenty-one (21) years of age.
- 2.16 Resource Family: The Resource Family provides care on a temporary (foster care) and/or permanent (adoption and legal guardianship) basis and includes all types of caregivers in the child welfare and probation systems formerly known as foster parents, approved relatives or approved Non-Relative Extended Family Member.
- 2.17 Special Incident Reports (SIRs): A confidential and formal written report following an incident at the FRC; the report must be submitted within twenty-four (24) hours of such incident.
- 2.18 Telehealth Services: Telehealth services which must be conducted subject to the State of California Board of Behavioral Sciences (BBS) Standards of Practice statutes and regulations for Telehealth, and in compliance with the Business and Professions Code 2290.5.

3. OUTCOME OBJECTIVES

CONTRACTOR shall meet the following goals and outcomes:

- 3.1 A minimum of seventy percent (70%) of PARTICIPANTS enrolled in Counseling

will complete services.

3.2 PARTICIPANTS who complete Counseling services will demonstrate improvement in parental resilience and knowledge of parenting and child development.

3.2.1 CONTRACTOR shall administer the Protective Factors Counseling Survey to PARTICIPANTS, as specified Subparagraph 16.5 of this Attachment A, at the initial face-to-face or virtual meeting and another upon completion or termination in the service, to determine if their parental resilience and knowledge of parenting and child development have improved as a result of the service.

3.3 A minimum of sixty percent (60%) of PARTICIPANTS enrolled in Parenting Education will complete services.

3.4 PARTICIPANTS enrolled in Personal Empowerment Program (PEP) will demonstrate improvement in parental resilience at post-test.

4. DESIGNATED LEAD AGENCY

4.1 Each of the Contractor Partner Agencies agrees that All For Kids Organization shall serve as the designated lead agent on behalf of the CONTRACTOR, with authority to present claims to COUNTY on behalf of each of the Contractor Partner Agencies for services delivered by each of them pursuant to this Contract. As designated lead agent, the CONTRACTOR shall receive the claims from each of the other Contractor Partner Agencies on a monthly basis and shall submit these claims, along with its own monthly claim, pursuant to Paragraph 20 of this Contract. Claims submitted to COUNTY by the designated lead agent shall clearly identify the services that were performed by Contractor Partner Agencies. Any and all payments to be made by COUNTY pursuant to this Contract shall be made payable to the designated lead agent. The designated lead agent shall thereafter disburse payment as appropriate to the Contractor Partner Agencies. Each of the Contractor Partner Agencies agrees that COUNTY's disbursement of payment to the designated lead agent shall satisfy COUNTY's payment obligation under this

Contract.

- 4.2 As the designated lead agent, All For Kids Organization shall also be responsible for activities that include, but are not limited to, the following:
- 4.2.1 Oversight of FRC services;
 - 4.2.2 Employment and supervision of the FRC Coordinator;
 - 4.2.3 Employment and/or oversight of the Community Engagement Coordinator;
 - 4.2.4 Establishing and facilitating a monthly FRC meeting with Contractor Partner Agencies and ensuring meetings minutes are documented;
 - 4.2.5 Coordinating weekly Case Management Team (CMT) meetings;
 - 4.2.6 Collecting and maintaining all invoice documentation;
 - 4.2.7 Overseeing the collection, maintenance, and management of all FRC data, including outcome measurements;
 - 4.2.8 Maintaining the integrity of the FaCT database and other reports, as necessary;
 - 4.2.9 Generating monthly reports (i.e., Service Grids) and other reports as requested, in accordance with Paragraph 36 of this Contract and Paragraph 10 of this Attachment A for submission to COUNTY;
 - 4.2.10 Overseeing and submitting to the COUNTY budget/contract modification requests on behalf of the FRC;
 - 4.2.11 Reimbursing FaCT-funded Contractor Partner Agencies for FaCT-funded services rendered prior to invoicing COUNTY;
 - 4.2.12 Producing, distributing, and maintaining a current, monthly FaCT FRC event/activity calendar as directed by ADMINISTRATOR;
 - 4.2.13 Coordinating FRC sustainability efforts referenced in Paragraph 17 of Attachment A;
 - 4.2.14 Ensuring Contractor Partner Agencies and/or subcontractor(s) are current on required documentation (e.g., insurance certificates, copies of resumes/applications, independent audits);
 - 4.2.15 Ensuring all non-FaCT funded partner agency(ies) have a current agreement with the FRC and provide copies of agreements to COUNTY

upon request;

- 4.2.16 Facilitating collaborative activities, services, and programs to ensure effective service delivery;
- 4.2.17 Submitting Special Incident Reports to the COUNTY; and
- 4.2.18 Attending required FaCT meetings and mandatory trainings as required by ADMINISTRATOR.

5. HOURS OF OPERATION

- 5.1 CONTRACTOR shall provide services during hours that are responsive to the needs of the population(s) to be served as determined by ADMINISTRATOR. At a minimum, CONTRACTOR shall provide FaCT core services for a minimum of eight (8) hours and thirty (30) minutes per day and shall remain open until at least 5:00 p.m., Monday through Friday.
- 5.2 CONTRACTOR shall also be available to provide FaCT core services during the evening hours, until at least 7:00 p.m., a minimum of two (2) days, Monday through Friday.
 - 5.2.1 CONTRACTOR may substitute a minimum of four (4) hours of delivery of FaCT core services on Saturday in lieu of the same number of evening hours provided Monday through Friday.
- 5.3 CONTRACTOR shall provide services during the following hours/days, able to be adjusted upon prior written approval from ADMINISTRATOR:

Monday	Tuesday	Wednesday	Thursday	Friday
11:00 a.m. – 7:30 p.m.	11:00 a.m. – 7:30 p.m.	9:00 a.m. – 5:30 p.m.	9:00 a.m. – 5:30 p.m.	9:00 a.m. – 5:30 p.m.

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

approval from ADMINISTRATOR for any closure outside of COUNTY's holiday schedule and the hours listed in Subparagraph 5.3 of this Attachment A. Any unauthorized closure shall be deemed a material breach of this Contract, pursuant to Paragraph 19, and shall not be reimbursed.

6. FRC GENERAL REQUIREMENTS AND CHARACTERISTICS

SSA, in partnership with community agencies, has embraced a model of community-based, family driven, collaborative service delivery. In keeping with these practices, SSA has adopted a nationally recognized model to frame outcomes and evaluation. Developed by the Center for Social Policy, the Strengthening Families model identifies five (5) Protective Factors ("Strengthening Families Protective Factors") described below have been identified in preventing the risk of child abuse and neglect. During the entire term of this Contract, CONTRACTOR shall:

6.1 Incorporate, into FaCT core services, the following five (5) Protective Factors:

- 6.1.1 Social Connections: Positive relationships that provide emotional, informational, instrumental, and spiritual support.
- 6.1.2 Knowledge of Parenting and Child Development: Understanding child development and parenting strategies that support physical, cognitive, language, and social/emotional development.
- 6.1.3 Social and Emotional Competence of Children: Family and child interactions that help children develop the ability to communicate clearly, recognize and regulate their emotions, and establish and maintain relationships.
- 6.1.4 Concrete Support in Times of Need: Access to concrete support and services that address a family's needs and help minimize stress caused by challenges.
- 6.1.5 Parental Resilience: Managing stress and functioning well when faced with challenges, adversity, and trauma.

6.2 Maintain a family-friendly community facility that functions as a multi-service community-based site that offers a "one-stop shop" approach to a comprehensive array of social and health services to families and provides a support system that

builds on family and community strengths.

- 6.3 Offer multiple programs, including, but not limited to, the following core services: a case management team, counseling, DR - Path Two, family support services, parenting education, domestic violence prevention and treatment (i.e., Personal Empowerment Program), and information and referral services in support of achieving FaCT goals.
- 6.4 Be situated in a community-based location easily accessed by pedestrians and within 880 yards (1/2 mile) of a bus stop or other form of affordable transportation.
- 6.5 Offer free and accessible parking.
- 6.6 Promote the FaCT platform (e.g., FRC sites, services, and literature) at a minimum of four (4) outreach events throughout the community, annually. Outreach efforts shall preferably target client demographics not currently served by the FRC.
- 6.7 Display FaCT literature representative of language composition within FRC lobbies and in areas accessible to PARTICIPANTS.
- 6.8 Involve local residents and stakeholders in planning, designing, implementing, and evaluating activities at the FRC.
- 6.9 Maximize the use of volunteers to assist not only in service delivery, but also serve as ambassadors in the community to promote community ownership and sustainability.
- 6.10 Leverage multiple funding streams to offer quality services to the community.
- 6.11 Operate as a collaborative that includes a minimum of three (3) FaCT funded Contractor Partner Agencies and a minimum of two (2) non-FaCT funded partner agencies who are providing onsite services at the FRC. Roles and responsibilities of each partner shall be clearly defined for the entire term of the Contract.
 - 6.11.1 Have each non-FaCT funded partner agency sign a memorandum of understanding or agreement specifying their commitment to provide

services throughout the term of this Contract.

- 6.12 Designate All For Kids Organization to function as both the designated lead agency and the program management lead agency. The fiscal and program management responsibilities shall include those referenced in Paragraph 4 of this Attachment A.
- 6.13 Provide bilingual direct service staff that are proportionate and culturally responsive to the language and cultural needs of the community they serve.
- 6.14 Collaborate with ADMINISTRATOR and COUNTY's FaCT Administrative Services provider, by attending required meetings, trainings, completing data entry into FaCT database system, and engaging with the FaCT Platform in activities related to the FaCT mission and vision.
- 6.15 Services shall be provided primarily in-person at the FRC, in-home, and/or in satellite sites such as schools and other community locations as mutually agreed upon by CONTRACTOR and ADMINISTRATOR. Virtual services may be offered based on PARTICIPANT's needs. Confidential space is required for all Family Support Services, Counseling, and CMT services.
- 6.16 Ensure PARTICIPANTS complete FaCT required registration, consent, sign-in forms, and/or complete assessment tools referenced in Subparagraph 16.5 of this Attachment A, when receiving services requiring an assessment.
- 6.17 Encourage 100% of PARTICIPANTS to complete satisfaction surveys when receiving FRC services.
- 6.18 Collaborate with COUNTY staff and COUNTY's contracted DR – Path Two services staff who provide services to PARTICIPANTS.
- 6.19 Provide information deemed necessary by SSA to complete any State-required reports related to services provided.

7. FRC SERVICE REQUIREMENTS

Throughout this Attachment A, Contractor Partner Agencies shall herein be referred to as: All for Kids Organization (AFK), Olive Crest (OC), and Human Options,

Inc. (HO). The Contractor Partner Agency that shall provide the particular service listed in Subparagraphs 7.1 through 7.9 below shall be indicated by the reference to that particular Contractor Partner Agency. Where more than one (1) Contractor Partner Agency is responsible for providing a service, or there is joint responsibility for providing the service, that responsibility will be outlined under the service category:

7.1 Case Management Team (OC)

7.1.1 The objectives of CMT services are as follows:

- 7.1.1.1 Increase collaboration among Contractor Partner Agencies by meeting on a weekly basis to effectively coordinate PARTICIPANT services;
- 7.1.1.2 Encourage family attendance and participation in determining their service needs;
- 7.1.1.3 Increase and facilitate resource linkages;
- 7.1.1.4 Improve individual and family functioning;
- 7.1.1.5 Decrease duplication of PARTICIPANT services; and
- 7.1.1.6 Foster the collaboration between the community, service providers, and FRCs to address the needs of children and families.

7.1.2 The CMT consists of an integrated multidisciplinary team, comprised of three (3) or more persons, trained and qualified to provide services. The CMT is responsible for identifying the educational, health, or social service needs of a child, and child's family, and for developing a plan to address these multiple needs as identified in Welfare and Institutions Code section 18986.40.

7.1.3 CONTRACTOR shall ensure participants of the CMT include all FaCT funded FRC service providers and non-FaCT funded agency representatives that would benefit the family.

7.1.4 CONTRACTOR shall ensure at a minimum, CMT participants shall include Counselor and Family Support Advocate.

7.1.5 CONTRACTOR shall encourage attendance of PARTICIPANTS referred to CMT.

- 7.1.6 CONTRACTOR and Contractor Partner Agencies shall jointly provide CMT services for a minimum of seventy-five (75) unduplicated FAMILIES annually. FRC CMT services include, but are not limited to: identifying the educational, health, or social service needs of a child and child's family; developing a plan to address these multiple needs; weekly reviews; team assessment; arranging and coordinating appropriate services; monitoring effectiveness of services; evaluating the outcome of services; and assigned clinician/intern, in conjunction with appropriate partners, will utilize clinical skills and knowledge of the community in order to access resources that are best suited to PARTICIPANT's needs. FRC CMT services shall include, but are not limited to, the following components:
- 7.1.6.1 Assessment: The CMT facilitator, based on input from the CMT, shall complete an assessment of PARTICIPANTS' strengths and needs.
- 7.1.6.2 Service Plan: On the basis of the assessment in Subparagraph 7.1.6.1, the CMT shall jointly develop an individualized service plan with the PARTICIPANT that identifies priorities, desired outcomes, strategies, and resources to be used in attaining the outcomes, follow up, and termination.
- 7.1.6.3 Reassessment: The CMT facilitator and CMT shall jointly reassess the PARTICIPANT's status, with input from Contractor Partner Agencies, in a weekly clinical review of cases. CMT meetings shall provide weekly evaluations and assessment for PARTICIPANTS.
- 7.1.6.4 Termination: The CMT facilitator and CMT shall jointly terminate the case from the CMT when the desired outcomes have been attained, the PARTICIPANT is non-compliant, or the PARTICIPANT withdraws.
- 7.1.7 CONTRACTOR and Contractor Partner Agencies shall jointly provide CMT services continuously throughout the term of this Contract. CMT

meetings shall be scheduled a minimum of one (1) day per week for a minimum of one (1) hour in duration. CMT meetings shall be held in an appropriate, private, and confidential space.

7.1.8 CMT meetings shall be facilitated by a qualified Counselor or staff person as specified in Subparagraph 14.2.3.2 of this Attachment A.

7.1.9 CONTRACTOR shall complete the CMT Tracking and Outcomes Log as well as the required forms referenced in Subparagraph 6.16 of this Attachment A.

7.2 Counseling Services (OC)

7.2.1 The objectives of Counseling Services are as follows:

7.2.1.1 Increase PARTICIPANT's coping skills;

7.2.1.2 Stabilize immediate crisis;

7.2.1.3 Increase access to social support systems;

7.2.1.4 Facilitate linkages to appropriate and needed treatment programs (e.g., domestic violence, substance use disorder, mental health, etc.);

7.2.1.5 Reduce risk of violence, abuse, and/or neglect in the home; and

7.2.1.6 Improve individual and family functioning.

7.2.2 CONTRACTOR shall utilize evidence-based practices to provide Crisis, Individual, Family, and Group Counseling Services for a minimum of four hundred (400) sessions annually.

7.2.2.1 A completed Crisis, Individual, Family, and Group Counseling session shall be counted as one (1) session regardless of number of PARTICIPANTS. A session shall be defined as a minimum of fifty (50) minutes in length.

7.2.2.2 A completed Group Counseling session exceeding ninety (90) minutes in length shall be counted as two (2) sessions regardless of the number of PARTICIPANTS. A Group Counseling session shall be sixty (60) to ninety (90) minutes each in duration.

7.2.3 CONTRACTOR Counseling Services shall be held primarily at the FRC, schools, or other mutually agreed upon community location, in an

appropriate, private, and confidential space; and be provided to PARTICIPANTS who are not covered by Medi-Cal or health insurance or who may be experiencing an immediate crisis that is disrupting their level of functioning.

7.2.4 Service Requirements per Modality:

7.2.4.1 Crisis Counseling Services: The duration of CONTRACTOR Crisis Counseling Services shall consist of a maximum of three (3) sessions for each PARTICIPANT.

7.2.4.2 Individual Counseling Services: CONTRACTOR shall provide Individual Counseling Services for a maximum of sixteen (16) sessions, for each PARTICIPANT. Additional sessions must be requested in advance and in writing for approval by ADMINISTRATOR. Individual Counseling sessions shall be offered to PARTICIPANTS on a weekly basis.

7.2.4.3 Family Counseling Services: CONTRACTOR shall provide Family Counseling Services for a maximum of sixteen (16) sessions, for each family. Additional sessions must be requested in advance and in writing for approval by ADMINISTRATOR. Family Counseling sessions may be weekly or daily, based on PARTICIPANTS' needs.

7.2.4.4 Group Counseling Services: The duration of Group Counseling Services shall consist of a minimum of four (4) group counseling series, with a minimum of four (4) to a maximum of sixteen (16) sessions per series. A session shall be sixty (60) to ninety (90) minutes each in duration.

7.2.5 CONTRACTOR shall provide in-person counseling services during FRC operating hours and on days and times that are responsive to the needs of the community, including evenings and weekends. Counseling Services may be provided via Telehealth Services as requested by PARTICIPANT or if held outside regular FRC hours.

7.2.6 CONTRACTOR shall provide qualified, bilingual Counselor staff as

specified in Subparagraph 14.2.5 of this Attachment A. CONTRACTOR Counselor staff shall attend all CMT meetings.

7.3 Differential Response – Path Two (DR-Path Two) (AFK)

The primary goal of DR-Path Two Services is to engage a greater number of families in services within the community without further child welfare intervention and, at the same time, reduce the recurrence of child maltreatment.

7.3.1 The objectives of DR-Path Two Services are as follows:

- 7.3.1.1 Support the family while in crisis;
- 7.3.1.2 Collaborate with COUNTY social worker and the family to devise a plan that identifies resources in an effort to protect the children and preserve the family;
- 7.3.1.3 Assess the family's needs, stabilize immediate crisis, and increase coping skills and family cohesiveness;
- 7.3.1.4 Develop a treatment plan to address individual and family needs to be offered for a minimum of thirty (30) days;
- 7.3.1.5 Provide in-home services, as needed, to address positive parenting skills, discipline, child development, and child health and safety; and
- 7.3.1.6 Present DR-Path Two cases at the CMT.

7.3.2 CONTRACTOR's DR-Path Two services shall focus on a family centered approach to: maintain children safely in the home; reduce entry into the child welfare system; serve as a support to families while in crisis; assess safety concerns and family's willingness to participate; provide team home visit; complete comprehensive family assessment; develop an individualized, needs based, and collaborative service plan; make referrals to community resources as appropriate; create linkage to assistance with service receipt; provide ongoing support; engage in advocacy; provide case management; provide ongoing tracking; follow up with family; provide assistance in accessing community resources; work with DR-Path Two COUNTY social worker(s) to ensure appropriateness of service plan in meeting goals while protecting children; and refer to CMT, facilitate

attendance, and include, at the family's request, extended family, non-family, and community leaders such as pastors/religious leaders as a long term support for family.

7.3.3 CONTRACTOR shall provide DR-Path Two Services during FRC operating hours. CONTRACTOR may also schedule evening hours at the request of the PARTICIPANTS.

7.4 Emergency Assistance (AFK)

The objective of Emergency Assistance (EA) services is to help stabilize families in crisis due to inability to meet their basic needs.

7.4.1 CONTRACTOR shall provide EA services for a minimum of thirty (30) FAMILIES annually.

7.4.2 EA services shall include an assessment of emergency needs and promote family self-sufficiency. The assessment shall be completed by qualified FRC staff and include recommendation(s) to meet the emergency needs of the PARTICIPANTS and a plan on how to circumvent the circumstances that lead to the crisis. Recommendations for use of EA funds shall be in accordance with Subparagraph 8.4 of Attachment A.

7.4.3 CONTRACTOR shall provide EA services primarily at the FRC and other community locations, as needed. Services shall be offered during FRC hours of operation or at dates and times convenient for the PARTICIPANT. CONTRACTOR shall provide EA services continuously throughout the term of this Contract.

7.4.4 CONTRACTOR shall complete the required forms referenced in Subparagraph 6.16 of Attachment A and the EA Tracking Log.

7.5 Family Support Services (AFK)

Family Support Services shall be provided to families with a minimum of two (2) core service needs. Services are provided through a collaborative process that assesses, plans, implements, coordinates, monitors, and evaluates the options and services required to meet PARTICIPANT needs.

7.5.1 The objectives of Family Support Services are as follows:

- 7.5.1.1 Support effective coordination of services among service providers;
 - 7.5.1.2 Promote knowledge of, and provide linkages, to resources, services, and opportunities to improve self-sufficiency; and
 - 7.5.1.3 Support families in following through with recommended services.
- 7.5.2 CONTRACTOR shall provide Family Support Services for a minimum of one hundred (100) unduplicated FAMILIES annually. Family Support Services are those services responsible for assessing the strengths and meeting the multiple needs of a PARTICIPANT and family; arranging, coordinating, monitoring, evaluating, and advocating for multiple services for families; and linking PARTICIPANTS to resources, services, and opportunities. The Family Support Advocate shall also teach and empower families to access community resources and strengthen problem solving skills.
- 7.5.3 CONTRACTOR shall provide Family Support Services continuously throughout the term of this Contract during FRC operating hours or on evenings as required by families. CONTRACTOR shall provide Family Support Services for a minimum of thirty (30) days per FAMILY.
- 7.5.4 CONTRACTOR shall provide Family Support Services primarily at the FRC, in the family's home, or at other community locations as agreed upon by PARTICIPANT.
- 7.5.5 CONTRACTOR shall provide qualified, bilingual Family Support Advocate staff as specified in Subparagraph 14.2.6 of this Attachment A. Family Support Advocate staff shall attend all FRC CMT meetings.
- 7.6 Information and Referral Services (AFK)
 - 7.6.1 The objective of Information and Referral Services is to increase access to community resources for families in need.
 - 7.6.2 Services include an assessment of need and referral services, including, but not limited to, the following: emergency housing, emergency food, counseling, childcare, substance abuse counseling and treatment,

parenting education, utility assistance, health and mental health treatment, education and job training, legal aid, and youth academic and recreation services. Information and Referral Specialist shall collaborate with other community agencies by receiving and referring PARTICIPANTS.

- 7.6.3 Information and Referral Specialist shall be stationed at the FRC reception area as the first point of contact for walk-in and telephone/email inquiries during FRC operating hours.
- 7.6.4 CONTRACTOR shall track Information and Referral Services using the FRC Daily Information and Referral Tracking Log to capture number of PARTICIPANTS served, PARTICIPANT zip code, mode of contact (e.g., phone call, walk-in, internet), and service(s) referred.
- 7.6.5 CONTRACTOR shall provide qualified, bilingual Information and Referral Specialist staff as specified in Subparagraph 14.2.8 of this Attachment A.

7.7 Parenting Education (OC)

- 7.7.1 The objectives for Parent Education are as follows:
 - 7.7.1.1 Provide social support;
 - 7.7.1.2 Enhance coping skills;
 - 7.7.1.3 Improve knowledge of child development; and
 - 7.7.1.4 Improve knowledge of appropriate and effective discipline.
- 7.7.2 CONTRACTOR shall provide evidence-based parenting curriculum as listed on the California Evidence Based Clearinghouse website (CEBC4CW.org). Elements of an effective parenting education program shall improve parenting skills and family functioning by teaching parents/caregivers about child development (e.g., developmental expectations), behavior management (e.g., discipline techniques), and coping skills (e.g., communication and stress management). As applicable, parenting education emphasis shall be placed on the prevention of recurrence of maltreatment and/or shall address attachment, bonding, and traumatic loss issues.
- 7.7.3 CONTRACTOR shall provide Parenting Education services for a

- minimum of thirty-two (32) unduplicated PARTICIPANTS annually.
- 7.7.4 CONTRACTOR shall provide a minimum of four (4) Parenting Education series annually. Frequency and length of each parenting series will be based on the selected evidence-based curriculum.
- 7.7.5 Parenting Education services shall be provided continuously during the term of this Contract at dates and times convenient for PARTICIPANTS. Services shall be offered at the FRC, schools, and other community locations as needed and approved by ADMINISTRATOR. A minimum of one (1) class shall be offered in-person at the FRC, annually.
- 7.7.6 CONTRACTOR shall ensure completion of required paperwork when providing parenting education to PARTICIPANTS receiving child welfare services, including, but not limited to, verification of attendance, issuance of certificates of completion, and verbal and/or written reports to COUNTY social workers.
- 7.7.7 CONTRACTOR shall provide parenting education in English and Spanish, or other language(s) that meet the needs of the community.
- 7.7.8 CONTRACTOR shall provide parenting instructors that are trained and certified to provide the selected evidence-based curriculum.
- 7.8 Personal Empowerment Program (Certified Domestic Violence Prevention and Treatment Education Program) (HO)
- 7.8.1 The objectives of Personal Empowerment Program (PEP) are as follows:
- 7.8.1.1 Raise awareness of the various types of domestic violence and its short and long term effects;
- 7.8.1.2 Develop or enhance safety plan for domestic violence victims;
- 7.8.1.3 Increase victim's understanding of the effects domestic violence has on children; and
- 7.8.1.4 Promote safety and permanency in homes and communities through prevention efforts aimed at child abuse and domestic violence.
- 7.8.2 CONTRACTOR shall provide PEP services to a minimum of forty-five (45) unduplicated PARTICIPANTS annually.

- 7.8.3 PEP services shall be an evidence-based ten (10) week educational support program designed to help victims break the cycle of domestic violence through education on the dynamics of domestic violence, effects of violence on victims and their children, and to help victims protect children who live in domestic violence homes. Topics shall include, but not be limited to, safety planning, boundaries, anger management, legal aspects of domestic violence, working through denial, and maintaining healthy relationships.
 - 7.8.4 CONTRACTOR shall provide PEP services continuously during the term of this Contract.
 - 7.8.5 During the entire term of this Contract, PEP providers must be approved by the PEP Program Collaborative of Orange County.
 - 7.8.6 CONTRACTOR shall offer PEP services at the FRC and other community locations at dates and times convenient for PARTICIPANTS and as approved by ADMINISTRATOR. CONTRACTOR may refer PARTICIPANTS to attend PEP services at any CONTRACTOR facilitated location that fits their language preference and schedule availability.
 - 7.8.7 PEP instructors shall administer the FaCT-approved pre/post measurement tools and enter the results into the FaCT database.
 - 7.8.8 CONTRACTOR shall ensure completion of required paperwork when providing PEP to PARTICIPANTS receiving child welfare services, including, but not be limited to, verification of attendance, issuance of certificates of completion, and verbal and/or written reports to COUNTY social workers.
- 7.9 Other Services (AFK)
- 7.9.1 Life Skills Workshops
 - 7.9.1.1 Life Skills Workshop services shall include, but not be limited to, the following topics: self-esteem and character building, increased coping skills and family bonding, issues facing children and teens, stress management, mindfulness, healthy

habits, and the impact of family trauma, child abuse, and domestic violence.

7.9.1.2 AFK shall provide Life Skills Workshop services to a minimum of fifty (50) PARTICIPANTS annually.

7.9.1.3 Life Skills Workshop services shall be provided in English and Spanish in a family-friendly, culturally responsive manner as participants need.

7.9.1.4 7.9.1.4 AFK shall ensure Life Skills Workshops are provided by quality staff.

7.9.2 Food Distribution Program

7.9.2.1 AFK shall oversee a monthly volunteer Food Distribution Program, which shall provide nutritious food staples to the community.

7.9.2.2 AFK shall distribute food to a minimum of seventy-five (75) PARTICIPANTS monthly.

7.9.2.3 AFK staff shall oversee FRC volunteers providing the service to all individuals in need and shall not discriminate based on race, color, national origin, sex, age, disability, or reprisal or retaliation for prior civil rights activity.

8. ADDITIONAL CONTRACTOR RESPONSIBILITIES

8.1 Provide a minimum of three (3) non-FaCT funded onsite services. Each non-FaCT funded service provider must have a signed MOU or contract specifying the commitment to provide services for the duration of the resulting contract term. CONTRACTOR shall provide copy of signed MOU to ADMINISTRATOR upon request.

8.2 Provide ADMINISTRATOR a detailed marketing plan for each contracted service, and revise, if necessary, as requested by ADMINISTRATOR.

8.3 Actively engage the community, including local residents, faith-based groups, businesses, public and private organizations, civic groups, and others in the

planning and implementation of services that promote the well-being, safety, and permanency of children, families, and communities.

- 8.4 CONTRACTOR shall use EA funds to meet the basic needs of PARTICIPANTS in support of services as described herein. Allowable costs include emergency food, emergency clothing, diapers, medicine, hygiene items, household items, transportation payment assistance, safety items, housing payment assistance and utility payment assistance, or other allowable costs, as approved in advance by ADMINISTRATOR. All purchases from EA funds in excess of five hundred dollars (\$500) per family must be requested in advance and in writing for approval by ADMINISTRATOR. Housing payment assistance and utility payment assistance in excess of one thousand dollars (\$1,000) per family shall be provided no more than one (1) time per fiscal year for each family, or as approved in advance and in writing by ADMINISTRATOR. CONTRACTOR shall research available community resource options prior to utilizing EA funds.
- 8.5 Develop and maintain a Governance Structure document outlining resource sharing, accountability, decision-making strategies, and conflict resolution plan. The Governance Structure shall include, but not be limited to, the addition and/or deletion of any Contractor Partner Agency and/or subcontractor(s), ongoing community input and involvement, and voting quorum (including what constitutes a quorum). FRC shall review and submit governance structure to ADMINISTRATOR by August 1st of each subsequent COUNTY fiscal year.
- 8.6 Develop a CEAC program that shall meet at least quarterly during the term of this Contract. CEAC shall develop and advance a community agenda to affect community level change. The FRC shall maintain a roster and a copy of minutes for all CEAC meetings. CEAC shall consist of community members such as parents, youths, teachers, school community liaisons, businesses professionals, religious community leaders, law enforcement, human and health service professionals, and city representatives. The composition of CONTRACTOR's CEAC shall vary, depending on the specific goals of, and the services to be

provided by the FRC. On an annual basis, CEAC shall assess, survey, and identify community strengths and needs to advocate for FRC services to meet community need; develop parent and youth leadership; and engage business community to provide tangible support and leadership. CEAC shall enlist broad community support and advocacy for the FRC by fundraising for the FRC and hosting events. A minimum of five hundred dollars (\$500) shall be allocated to the CEAC within the FRC budget for the purposes of its members to use for planning events, and other activities as deemed necessary by CEAC. CONTRACTOR shall provide a qualified Community Engagement Coordinator staff as specified in Subparagraph 14.2.4 of this Attachment A.

- 8.7 Follow procedures provided by ADMINISTRATOR for reporting any special incidents that occur during CONTRACTOR's performance of duties under this Contract, involving CONTRACTOR's staff, PARTICIPANTS, and/or property.
- 8.8 CONTRACTOR shall provide childcare services at the FRC to children of parents attending FRC programs during FRC operating hours, continuously throughout the term of this Contract, at dates and times convenient for PARTICIPANTS. Allowable costs include direct childcare services and purchases of cleaning supplies, snacks directly related to childcare services, activities, age appropriate toys, crafts, and games. Childcare services shall be reimbursed based on actual hours worked. CONTRACTOR shall provide childcare staff that are at least eighteen (18) years of age; possess a high school diploma or equivalent; have one (1) year of child care experience; possession of, or ability to obtain a valid Pediatric CPR and First Aid Certification prior to providing child care duties; and ability to deal with stressful situations.

9. FACILITIES

- 9.1 FRC is located at:
Oak View Family Resource Center
17261 Oak Lane
Huntington Beach, CA 92647

9.2 Administrative services under this Contract shall be provided at:

All For Kids Organization

1910 Magnolia Ave.

Los Angeles, CA 90007

CONTRACTOR shall provide facility(ies) for administering FRC Services. CONTRACTOR's facilities shall be safe, clean, and maintained in compliance with all applicable laws, rules, regulations, building codes, statutes, and orders, as they now exist or may be subsequently amended.

10. REPORTING REQUIREMENTS

CONTRACTOR shall prepare and submit written reports in a format approved in writing by ADMINISTRATOR. Written reports include the Quarterly Assessment Report and the Monthly Service Grid.

10.1 Monthly Service Grid Reports shall be submitted to ADMINISTRATOR by the twentieth (20th) day of each month for the preceding month of services. In the event the twentieth (20th) calendar day falls on a weekend or COUNTY holiday as specified in Subparagraph 5.4 of this Attachment A, CONTRACTOR shall submit the Monthly Service Grid the next business day. Monthly Service Grid Reports shall be complete and reflect services provided in prior month.

10.2 Quarterly Assessment Reports shall be submitted quarterly to ADMINISTRATOR by the twentieth (20th) day of the quarter month. In the event the twentieth (20th) calendar day falls on a weekend or COUNTY holiday as specified in Subparagraph 5.3 of this Attachment A, CONTRACTOR shall submit the Quarterly Assessment Report the next business day. Quarterly Assessment Reports shall be complete and reflect assessments completed in each quarter.

10.3 CONTRACTOR shall complete the FaCT standardized Marketing Outreach Log and CEAC Data Form, and shall submit to ADMINISTRATOR quarterly, ten (10) calendar days following the end of each quarter.

10.4 CONTRACTOR shall provide information deemed necessary by ADMINISTRATOR to complete any state-required reports related to the services

provided under this Contract.

11. MEETINGS

- 11.1 CONTRACTOR shall ensure the FRC Coordinator participates in meetings of all FaCT FRC Coordinators for the purpose of information sharing, joint problem solving, identification of Best Practices, development of common approaches to case management and intake, training, and other related matters. Meetings will occur a minimum of one (1) time per month. ADMINISTRATOR will provide CONTRACTOR with detailed information regarding meeting date(s) and location(s).
- 11.2 CONTRACTOR shall ensure appropriate CONTRACTOR staff participates in all required meetings as identified by ADMINISTRATOR. ADMINISTRATOR will provide CONTRACTOR with detailed information regarding meeting date(s) and location(s).

12. UTILIZATION REVIEW

- 12.1 CONTRACTOR and ADMINISTRATOR's designee shall meet to review and evaluate a random selection of family case records. The review may include, but is not limited to, an evaluation of the necessity and appropriateness of services provided and length of services. Family cases to be reviewed shall be randomly selected by ADMINISTRATOR and may include both open and closed cases.
- 12.2 ADMINISTRATOR may conduct a Utilization Review (UR) at CONTRACTOR's facility referenced in Paragraph 9 of this Attachment A, with date and time determined at ADMINISTRATOR's discretion. ADMINISTRATOR may provide oral and/or written feedback regarding the UR findings. CONTRACTOR shall comply with the findings of the UR and take corrective action accordingly.
- 12.3 In the event CONTRACTOR, ADMINISTRATOR and COUNTY's CFS staff representatives and/or ADMINISTRATOR's designee are unable to resolve differences of opinion regarding the necessity and appropriateness of services and length of services, the dispute shall be submitted to COUNTY's CFS Director for

final resolution. Nothing in this subparagraph shall affect COUNTY's termination rights under Paragraph 41 of this Contract.

13. BUDGET

13.1 CONTRACTOR shall provide the following described staff positions continuously throughout the term of the Contract, at the specified Full-Time Equivalent (FTE):

Position Title	Position Type ⁽¹⁾	FTE Minimum ⁽²⁾	Max Hourly Rate ⁽³⁾
Administrative Assistant	A	0.05 FTE	\$23.00
Clinical Supervisor	A	0.05 FTE	\$44.00
CMT Facilitator	A	0.05 FTE	\$44.00
Community Engagement Coordinator	D	0.25 FTE	\$24.50
Counselor	D	0.50 FTE*	\$35.50
Family Support Advocate	D	1.0 FTE	\$29.00
FRC Coordinator	D	1.0 FTE	\$37.50
Information and Referral Specialist	D	1.0 FTE	\$27.00
Program Manager	A	0.12 FTE	\$55.63

*0.10 FTE will be in-kind.

13.2 The budget for services provided pursuant to Attachment A of this Contract is set forth as follows:

FRC Services	Year One (7/1/25 – 6/30/26)	Year Two (7/1/26 – 6/30/27)	Year Three (7/1/27 – 6/30/28)
Direct Service Costs ^(1,2,3,4,5)	\$324,517	\$324,517	\$324,517
Indirect Costs ⁽⁶⁾	\$25,483	\$25,483	\$25,483
Total Maximum Obligation	\$350,000	\$350,000	\$350,000

⁽¹⁾ Position Types are classified as "D" for Direct or "A" for Administrative. Direct services positions include staff who are integral to service delivery and may include staff who provide direct face-to-face service to clients and/or staff who supervise/manage direct service personnel. Administrative positions include staff that support service delivery and whose activities and functions can be directly allocated to the program.

(2) For hourly employees, Full-Time Equivalent (FTE) is defined as the amount of time (stated as a percentage) the position will be providing services under the terms of this Contract. This percentage is based upon a 40-hour work week. For salaried employees, FTE is defined as the amount of time (stated as a percentage) the position will be paid for under the terms of this Contract, regardless of the number of hours actually worked.

(3) Maximum hourly rate which will be permitted during the term of this Contract; employees may be paid at less than maximum hourly rate. Total salary is based on estimated cost, not maximum hourly rate.

(4) Employee Benefits include contributions to 401k or retirement plans; health insurance; dental insurance; vision insurance; life insurance; long-term disability insurance; payroll taxes such as FICA, Federal Unemployment Tax, State Unemployment Tax, and Workers' Compensation Tax, based on the currently prevailing rates; CONTRACTOR's benefits and expense for accrued vacation time payout, for a separated employee, limited to the actual vacation time accrued during the fiscal year in which the expense is claimed, minus the actual vacation time used by the employee during said fiscal year. The overall benefit rate shall not exceed 29% of the actual salary expense claimed.

(5) Mileage is limited to the amount allowed by IRS.

(6) Indirect cost includes administrative cost not directly charged to the program including Accounting, Human Resources, Facilities, Information Technology, and Information Systems departments. Indirect costs are based on 10% of total direct costs. In the event the indirect cost rate is reduced, the reduction shall be afforded to ADMINISTRATOR and the budget amended accordingly. CONTRACTOR shall provide notification to ADMINISTRATOR of any changes in the rate.

13.3 Expenses for extra pay, including but not limited to, overtime, stipends, bonuses, staff incentives, severance pay, etc. shall not be eligible for reimbursement under this Contract unless authorized in writing by ADMINISTRATOR. Such authorization shall be considered as an exception and may be approved, on a case-by-case basis, at the sole discretion of ADMINISTRATOR.

13.4 CONTRACTOR and ADMINISTRATOR may agree, subject to advance written notice, to add, delete or modify line items and/or amounts and/or the number and

type of FTE positions without changing COUNTY's maximum funding obligation as stated in Subparagraph 20.1 of this Contract or reducing the level of service to be provided by CONTRACTOR. Further, in accordance with Subparagraph 41.4 of this Contract, in the event ADMINISTRATOR reduces the maximum funding obligation as stated in Subparagraph 20.1, CONTRACTOR and ADMINISTRATOR may mutually agree in writing to proportionately reduce the service goals as set forth in this Attachment. Failure to obtain advance written approval for any proposed Budget Modification Request may result in disallowance of reimbursement for those costs.

- 13.5 In the event the budget shown in Subparagraph 13.2 of this Attachment A is modified, the modified budget shall remain in effect for the remainder of the contract term, unless superseded by subsequent budget modification(s) that have been approved in writing by ADMINISTRATOR. For example, if Budget Modification #1 is approved on August 15, 2025, the modified budget will remain in effect until Budget Modification #2 is requested and approved in writing. The annual budget beginning on July 1st of each Contract year shall be identical to the most recently modified annual budget.

14. STAFFING REQUIREMENTS

14.1 Recruitment Practices

- 14.1.1 CONTRACTOR shall use a formal recruitment plan which complies with federal and State employment and labor regulations. CONTRACTOR shall recruit and maintain trained personnel who are responsive to, and who understand, the diversity of cultures which can be found among the target population identified in Paragraph 1 of this Attachment A. CONTRACTOR shall employ staff with the background, education, training, language skills, and experience to perform all functions as described in this Contract.
- 14.1.2 CONTRACTOR shall notify ADMINISTRATOR, in writing, no later than seventy-two (72) hours of any staffing vacancies or filling of vacant positions that occur during the term of this Contract. For resignations,

CONTRACTOR's notification shall include employee's name, position title, date of resignation, a description of planned recruitment activities, and the CONTRACTOR's contingency plan to cover services during the vacancy. For new hires, CONTRACTOR's notification shall include candidate's resume or application, position title, and date of hire.

14.1.3 The number of direct service bilingual staff proposed should include how staffing will meet the needs of the community to be served.

14.1.4 CONTRACTOR may be required to submit employer's bilingual certification criteria and/or test results to ADMINISTRATOR.

14.2 CONTRACTOR shall provide the following described staff positions continuously throughout the term of the Contract, at the specified Full-Time Equivalent (FTE):

14.2.1 Administrative Assistant (OC)

Duties

14.2.1.1 Prepare reports, invoices, and charts; collate data related to client services delivered.

Qualifications

14.2.1.2 High School Diploma. Course work in computers, Outlook, Excel, Databases. Proficiency in English is required. Based on community need, bilingual proficiency may be required.

14.2.2 Clinical Supervisor (OC)

Duties

14.2.2.1 Provide clinical supervision to counselors; review caseload, documentation, and assessments; provide guidance for varying modalities.

Qualifications

14.2.2.2 Licensed clinician registered with the State of California Department of Consumer Affairs, Board of Behavioral Sciences (BBS) or Board of Psychology. Master's degree in Clinical Social Work. Must have relevant training in Trauma Informed Care, Motivational Interviewing, Family Systems, and Cognitive Behavioral Therapy. Responsible for the supervision of all

associates and interns in accordance with BBS requirements.

14.2.3 CMT Facilitator (OC)

Duties:

14.2.3.1 Facilitate CMT group process, ensure thorough assessment and linkages for families to resources, and ensure team and/or staff members follow up on all mandated reporting requirements. Responsibilities include, but are not limited to: verify and track attendance of required CMT members; ensure PARTICIPANT confidentiality/release forms are signed by PARTICIPANT and CMT members; review the laws of confidentiality and child and elder/dependent adult abuse reporting on an annual basis, and ensure compliance for each case presented; ensure all CMT cases conferenced are multiple needs cases (i.e., client needs Counseling and PEP); facilitate weekly review of CMT cases, including a thorough assessment of needs, service plan, follow up plan, and termination; encourage staff to invite FAMILIES to the CMT meetings; maintain weekly case logs and registration forms for each case conferenced at CMT; complete standardized CMT assessment tools, ensuring COUNTY required CMT data is accurately entered into FaCT database; and actively engage new collaborative partners and/or other COUNTY agency representatives to conference cases that would benefit families.

Qualifications

14.2.3.2 Counselor or staff person with a minimum of one (1) year of group/meeting facilitation experience and ability to perform CMT Facilitator duties specified in Subparagraph 14.2.1 of this Attachment A. Proficiency in English is required.

14.2.4 Community Engagement Coordinator (AFK)

The Community Engagement Coordinator shall not be a current member of the CEAC.

Duties

14.2.4.1 Assist in advocacy for the expansion of the FRC CEAC and Youth Action Council (YAC) programs and activities focusing on issues that affects the health, well-being, and public safety of residents in the FRC community; develop CEAC leadership and recruit and sustain CEAC and/or YAC membership; provide direct technical assistance and support to CEAC; oversee community organizing, volunteer recruitment and training, problem solving, and developing and implementing an outreach plan; support the efforts of local programs to explore donation and service opportunities for the FRC; develop and promote FRC volunteer service project activities; develop and maintain regular contact with community organizations and local schools; coordinate and communicate with FRC Coordinator; attend all required meetings and trainings; administer FaCT-approved measurement tools; and enter the results into the FaCT database.

Qualifications

14.2.4.2 Option One (1): An Associate's degree or sixty (60) college units in human services or related field from an accredited college/university; one (1) year of experience, including leadership/supervisory experience, providing direct services to the target population; capable of relating well to individuals from diverse backgrounds, cultures, varied income, and education levels; and computer competency. Proficiency in English is required. Based on community need, bilingual proficiency may be required; or

Option Two (2): Three (3) years of experience, including one (1) year of leadership/supervisory experience, providing direct services to the target population; capable of relating well to individuals from diverse backgrounds, cultures, varied income, and education levels; and computer competency. Proficiency in English is required. Based on community need, bilingual

proficiency may be required.

14.2.5 Counselor (OC)

Duties

14.2.5.1 Provide therapy, including assessment, treatment planning, termination, and documentation; communicate applicable case related information to SSA staff, as requested; attend weekly CMT meetings; and complete FaCT designated measurement tools and enter all required data into the FaCT database.

Qualifications

14.2.5.2 Licensed clinician registered with the State of California Department of Consumer Affairs, Board of Behavioral Sciences (BBS); or graduate behavioral science degree intern. All associates and interns must be receiving direct clinical supervision in accordance with BBS requirements. It is the responsibility of the licensed clinical supervisor to ensure that the extent, kind, and quality of clinical services performed is consistent with the training and experience of the associate and/or intern. Proficiency in English is required. Based on community need, bilingual proficiency may be required.

14.2.6 Family Support Advocate (AFK)

Duties

14.2.6.1 Responsible for serving all Family Support Services referrals. Services shall include, but not limited to: assessing family strengths and needs; linkages to resources; case planning; in-home services; communicating applicable case related information to SSA staff, as requested; compiling and maintaining records; preparing reports; presenting cases at CMT meetings; completing FaCT designated measurement tools and entering all required data into the FaCT database; and attending all required FaCT meetings and trainings.

Qualifications

14.2.6.2 Option One (1): Bachelor's degree in human services or related field from an accredited university. Proficiency in English is required. Based on community need, bilingual proficiency may be required; or

Option Two (2): A minimum of three (3) years of experience providing direct services to the target population. Proficiency in English is required. Based on community need, bilingual proficiency may be required.

14.2.7 FRC Coordinator (AFK)

Duties

14.2.7.1 FRC Coordinator's work schedule shall be consistent with FRC operating hours and their workspace shall be located at the FRC. Perform a variety of administrative functions, including: coordinate service providers; supervise FRC staff; oversee the day-to-day operation of the FRC; compile statistical and financial data for various reports; prepare and monitor program budget; coordinate governance and policy procedure development; coordinate training opportunities for staff; provide community involvement opportunities for CEAC; perform outreach to community businesses and schools; market FRC services within the community; initiate outreach to new partners and service providers; address public inquiries regarding services, procedures, operations and regulations; facilitate FRC partners and staff meetings and ensure completion of meeting minutes; complete all required documentation; attend required FaCT meetings and trainings; and perform related duties as assigned.

Qualifications

14.2.7.2 Option One (1): Bachelor's degree (Master's degree preferred) in social work, sociology, psychology, or related field from an accredited university and two (2) years of experience providing direct services to the target population; a minimum of one (1)

year of leadership and/or supervisory experience; capable of relating well to individuals from diverse backgrounds, cultures, varied income, and education levels; ability to work successfully in a collaborative environment; attention to detail; and computer competency. Proficiency in English is required. Based on community need, bilingual proficiency may be required; or

Option Two (2): A minimum of five (5) years of experience providing direct services to the target population in progressively responsible roles; a minimum of one (1) year of leadership and/or supervisory experience; capable of relating well to individuals from diverse backgrounds, cultures, varied income, and education levels; ability to work successfully in a collaborative environment; attention to detail; and computer competency. Proficiency in English is required. Based on community need, bilingual proficiency may be required.

14.2.8 Information and Referral Specialist (AFK)

Duties

14.2.8.1 Respond to walk-in, call-in, and referred PARTICIPANTS seeking community resources; assess PARTICIPANTS's immediate needs and make referrals to appropriate resources; and track referrals on Information and Referral Tracking Log and enter into the FaCT database.

Qualifications

14.2.8.2 High school diploma or equivalent, one (1) year of customer service experience working directly with the public, and computer competency (i.e., knowledge and ability to use computers and related technology). Proficiency in English is required. Based on community need, bilingual proficiency may be required.

14.2.9 Program Manager (AFK)

Duties

14.2.9.1 Responsible for administrative and budgetary oversight of County of Orange SSA (FaCT) contracts at designated sites; leadership and supervisory support including staff development plans to ensure contract goals are met; oversee FRC projects and initiatives; collaborate with FaCT leadership; attend FaCT committee meetings and forums, and local and regional FRC platform advocacy.

Qualifications

14.2.9.2 Option One (1): A Master's degree from an accredited college/university with two (2) years of management experience; four (4) years of increasingly responsible recreation/grant program experience, including one (1) year of lead supervisory responsibility; or

Option Two (2): A Bachelor's degree or equivalent to a bachelor's degree from an accredited college/university with major course work in recreation, public administration or a related field; five (5) years management experience; four (4) years of increasingly responsible recreation/grant program experience, including one (1) year of lead supervisory responsibility.

15. TRAINING

- 15.1 CONTRACTOR shall ensure appropriate CONTRACTOR staff participates in all required trainings and/or meetings as identified by ADMINISTRATOR. ADMINISTRATOR will provide CONTRACTOR with detailed information regarding training/meeting date(s) and location(s).
- 15.2 Trainings eligible for reimbursement through this Contract must be approved in advance, in writing, by ADMINISTRATOR.
- 15.3 At the request of ADMINISTRATOR, CONTRACTOR shall attend trainings

presented or sponsored by COUNTY.

- 15.4 CONTRACTOR shall ensure that CONTRACTOR's staff receives cultural awareness and responsiveness training.

16. DATA ENTRY AND DATA SUBMISSION REQUIREMENTS

- 16.1 CONTRACTOR shall maintain data that includes the types and amounts of services provided to each PARTICIPANT, assessment data, and key demographic items, including, but not limited to: family identifier, family member identifier, ethnicity, date of birth, sex, referral reason(s), services recommended, services provided, date service delivery begins, date service delivery ends, status indicators (e.g., previous abuse reports, existing health problems), and primary language spoken.
- 16.2 CONTRACTOR shall be responsible for the integrity of all data. This includes ensuring all required PARTICIPANT and service data is entered and maintained in the FaCT database. Data for services incurred in the preceding month shall be available for review prior to the date of the regularly scheduled monthly steering committee meeting, or as requested by ADMINISTRATOR. Data includes monthly service grids, quarterly assessment reports, and other reports as required by ADMINISTRATOR.
- 16.3 Services provided at the FRC fall under one (1) or more of the Protective Factors, as defined in Paragraph 6 of this Attachment A. FaCT core services have their own measurement tool that shall be administered and used to collect data and entered into the FaCT database. The current FaCT database system is a web-based PARTICIPANTS management system, managed by FaCT and its administrative contractor, which provides contractual and outcome based reporting for each FRC. FRCs shall work closely with ADMINISTRATOR to maximize utility and adhere to confidentiality within the data system. FaCT shall provide technical assistance and training to the FRCs to ensure strong data collection and outcome reporting.
- 16.4 Direct service staff shall be responsible for entering PARTICIPANT service and outcome data for FaCT funded services into the FaCT database. These include, but

are not limited to, the following:

- 16.4.1 CMT Facilitator shall administer, collect, and enter the CMT tracking and assessment tool;
- 16.4.2 Family Support Advocate shall administer, collect, and enter the Family Development Matrix Tool(s);
- 16.4.3 Parenting Educator shall administer, collect, and enter the Parenting Education Survey; and
- 16.4.4 Direct service provider shall administer, collect, and enter the Registration Form.

- 16.5 In addition to the FaCT Registration form and/or FaCT Large Group Tracking form, the following assessment tool(s) are required for each core service include:

Core Services	Required Assessment Tool(s)
CMT	CMT Tracking & Outcomes Log
Counseling Services	Protective Factors Counseling Survey
Emergency Assistance Services	Emergency Assistance Tracking Log
Family Support Services	Family Development Matrix
Information & Referral Services	Information & Referral Tracking Log
Parenting Education	Protective Factors Parenting Survey
Personal Empowerment Program	PEP Pre/Post Test

- 16.6 The FRC Coordinator is responsible for ensuring data integrity and accurate data collection. FRC Coordinator shall also ensure that the data is entered correctly into the FaCT data system and within timelines required by ADMINISTRATOR. Contractor Partner Agencies are responsible for their own staff data collection, ensuring data integrity, and accurate submission to the FRC Coordinator.
- 16.7 FRCs can administer COUNTY-approved measurement tools (e.g., tracking logs, pre/post-tests, satisfaction surveys, etc.) to collect data on other services. ADMINISTRATOR shall provide CONTRACTOR a minimum of ten (10) business day notice in the event a measurement tool is changed.
- 16.8 The COUNTY measurement tools, referenced in Subparagraph 6.16 of this Attachment A, are subject to change based on program and evaluation needs as defined by ADMINISTRATOR.

17. SUSTAINABILITY

- 17.1 CONTRACTOR agrees to demonstrate, throughout the term of this Contract, the ability to integrate multiple public, private, and collaborative partner funding sources.
- 17.2 CONTRACTOR must provide measurable goals that demonstrate resource leveraging and in-kind partnerships and/or grants based on service gaps and identified needs, specific to the community.
- 17.3 CONTRACTOR agrees to work with ADMINISTRATOR in order to pursue long-term sustainability of CONTRACTOR's FaCT collaborative programs. This includes, but is not limited to, participation in the following:
- 17.3.1 Assessment of long-term need for and reasonableness of FaCT collaborative programs;
 - 17.3.2 Training programs developed by or for FaCT;
 - 17.3.3 Outreach activities initiated by FaCT staff or FaCT committees, as mutually agreed by CONTRACTOR and ADMINISTRATOR;
 - 17.3.4 Research of other public/private funding sources and opportunities;
 - 17.3.5 Pursuit of linkages with other partners, as appropriate; and
 - 17.3.6 Development of marketing and community education materials as mutually agreed upon by CONTRACTOR and ADMINISTRATOR.
- 17.4 CONTRACTOR agrees to cooperate in these efforts, as well as independently pursue opportunities to improve sustainability of their collaborative program. Independent activities may include activities identified above as well as grant writing and engaging in collaborative agreements with other integrated service initiatives.

18. QUALITY ASSURANCE/QUALITY CONTROL

- 18.1 CONTRACTOR shall utilize a comprehensive Quality Control Plan, on a format approved by the SSA, to monitor the level of program service and quality. The Quality Control Plan shall be effective upon Contract start date and will be updated and resubmitted for SSA approval when changes occur. The Quality Control Plan

will include, but not be limited to, the following:

- 18.1.1 The method for ensuring the services, deliverables, and requirements defined in the Contract are being provided at or above the level of quality per this Contract;
- 18.1.2 The method for assuring that the professional staff rendering services under this Contract has the necessary qualifications;
- 18.1.3 The method of identifying and preventing deficiencies in the quality of service as defined by COUNTY policy; and
- 18.1.4 The method for providing SSA with a copy of CONTRACTOR's case reviews, a clear description of, and corrective action taken, to resolve identified problems.

ATTACHMENT B

COUNTY OF ORANGE INFORMATION TECHNOLOGY SECURITY PROVISIONS

All Contractors with access to County data and/or systems shall establish and maintain policies, procedures, and technical, physical, and administrative safeguards designed to (i) ensure the confidentiality, integrity, and availability of all County data and any other confidential information that the Contractor receives, stores, maintains, processes, transmits, or otherwise accesses in connection with the provision of the contracted services, (ii) protect against any threats or hazards to the security or integrity of County data, systems, or other confidential information, (iii) protect against unauthorized access, use, or disclosure of personal or County confidential information, (iv) maintain reasonable procedures to prevent, detect, respond, and provide notification to the County regarding any internal or external security breaches, (v) ensure the return or appropriate disposal of personal information or other confidential information upon contract conclusion (or per retention standards set forth in the contract), and (vi) ensure that any subcontractor(s)/agent(s) that receives, stores, maintains, processes, transmits, or otherwise accesses County data and/or system(s) is in compliance with statements and the provisions of statements and services herein.

1. This County of Orange Information Technology Security Provisions document provides a high-level guide for contractors to understand the resiliency and cybersecurity expectations of the County. The County of Orange Security Guidelines follow the latest National Institute of Standards and Technology (NIST) 800-53 framework to ensure the highest levels of operational resiliency and cybersecurity.

Contractor, Contractor personnel, Contractor's subcontractors, any person performing work on behalf of Contractor, and all other agents and representatives of Contractor will, at all times, comply with and abide by all County of Orange Information Technology Security Provisions ("Security Provisions") that pertain to Contractor(s) in connection with the Services performed by Contractor(s) as set forth in the scope of work of this Contract. Any violations of the Security Provisions shall, in addition to all other available rights and remedies available to County, be cause for immediate termination of this Contract. Such Security Provisions include, but are not limited to, Attachment "D" - County of Orange Information Technology Security Guidelines.

Contractor shall use industry best practices and methods with regard to confidentiality, integrity, availability, and the prevention, detection, response, and elimination of threat, by all appropriate means, of fraud, abuse, and other inappropriate or unauthorized access to County data and/or system(s) accessed in the performance of Services under this Contract.

2. The Contractor shall implement and maintain a written information security program that contains reasonable and appropriate security measures designed to safeguard the confidentiality, integrity, availability, and resiliency of County data and/or system(s). The Contractor shall review and update its information security program in accordance with contractual, legal, and regulatory requirements. Contractor shall provide to County a copy of the organization's information security program and/or policies.

3. Information Access: Contractor shall use appropriate safeguards and security measures to ensure the confidentiality and security of all County data.

County may require all Contractor personnel, subcontractors, and affiliates approved by County to perform work under this Contract to execute a confidentiality and non-disclosure agreement concerning access protection and data security in the form provided by County. County shall authorize, and Contractor shall issue, any necessary information-access mechanisms, including access IDs and passwords, and in no event shall Contractor permit any such mechanisms to be shared or used by other than the individual Contractor personnel, subcontractor, or affiliate to whom issued. Contractor shall provide each Contractor personnel, subcontractors, or affiliates with only such level of access as is required for such individual to perform his or her assigned tasks and functions.

Throughout the Contract term, upon request from County but at least once each calendar year, Contractor shall provide County with an accurate, up-to-date list of those Contractor personnel and/or subcontractor personnel having access to County systems and/or County data, and the respective security level or clearance assigned to each such Contractor personnel and/or subcontractor personnel. County reserves the right to require the removal and replacement of Contractor personnel and/or subcontractor personnel at the County's sole discretion. Removal and replacement shall be performed within 14 calendar days of notification by the County.

All County resources (including County systems), County data, County hardware, and County software used or accessed by Contractor: (a) shall be used and accessed by such Contractor and/or subcontractors personnel solely and exclusively in the performance of their assigned duties in connection with, and in furtherance of, the performance of Contractor's obligations hereunder; and (b) shall not be used or accessed except as expressly permitted hereunder, or commercially exploited in any manner whatsoever, by Contractor or Contractor's personnel and subcontractors, at any time.

Contractor acknowledges and agrees that any failure to comply with the provisions of this paragraph shall constitute a breach of this Contract and entitle County to deny or restrict the rights of such non-complying Contractor personnel and/or subcontractor personnel to access and use the County data and/or system(s), as County in its sole discretion shall deem appropriate.

4. Data Security Requirements: Without limiting Contractor's obligation of confidentiality as further described in this Contract, Contractor must establish, maintain, and enforce a data privacy program and an information and cyber security program, including safety, physical, and technical security and resiliency policies and procedures, that comply with the requirements set forth in this Contract and, to the extent such programs are consistent with and not less protective than the requirements set forth in this Contract and are at least equal to applicable best industry practices and standards (NIST 800-53).

Contractor also shall provide technical and organizational safeguards against accidental, unlawful, or unauthorized access or use, destruction, loss, alteration, disclosure, transfer, commingling, or processing of such information that ensure a level of security appropriate to the risks presented by the processing of County Data,

Contractor personnel and/or subcontractor personnel and affiliates approved by County to perform work under this Contract may use or disclose County personal and confidential information only as permitted in this Contract. Any other use or disclosure requires express approval in writing by the County of Orange. No Contractor personnel and/or subcontractor personnel or affiliate shall duplicate, disseminate, market, sell, or disclose County personal and confidential information except as allowed in this Contract. Contractor personnel and/or subcontractor personnel or affiliate who access, disclose, market, sell, or use County personal and confidential information in a manner or for a purpose not authorized by this Contract may be subject to civil and criminal sanctions contained in applicable federal and state statutes.

Contractor shall take all reasonable measures to secure and defend all locations, equipment, systems, and other materials and facilities employed in connection with the Services against hackers and others who may seek, without authorization, to disrupt, damage, modify, access, or otherwise use Contractor systems or the information found therein; and prevent County data from being commingled with or contaminated by the data of other customers or their users of the Services and unauthorized access to any of County data.

Contractor shall also continuously monitor its systems for potential areas where security could be breached. In no case shall the safeguards of Contractor's data privacy and information and cyber security program be less stringent than the safeguards used by County. Without limiting any other audit rights of County, County shall have the right to review Contractor's data privacy and information and cyber security program prior to commencement of Services and from time to time during the term of this Contract.

All data belongs to the County and shall be destroyed or returned at the end of the contract via digital wiping, degaussing, or physical shredding as directed by County.

5. Enhanced Security Measures: County may, in its discretion, designate certain areas, facilities, or solution systems as ones that require a higher level of security and access control. County shall notify Contractor in writing reasonably in advance of any such designation becoming effective. Any such notice shall set forth, in reasonable detail, the enhanced security or access-control procedures, measures, or requirements that Contractor shall be required to implement and enforce, as well as the date on which such procedures and measures shall take effect. Contractor shall and shall cause Contractor personnel and subcontractors to fully comply with and abide by all such enhanced security and access measures and procedures as of such date.
6. General Security Standards: Contractor will be solely responsible for the information technology infrastructure, including all computers, software, databases, electronic systems (including database management systems, email systems, auditing, and monitoring systems) and networks used by or for Contractor ("Contractor Systems") to access County resources (including County systems), County data or otherwise in connection with the Services and shall prevent unauthorized access to County resources (including County systems) or County data through the Contractor Systems.

- a) **Contractor System(s) and Security:** At all times during the contract term, Contractor shall maintain a level of security with regard to the Contractor Systems, that in all events is at least as secure as the levels of security that are common and prevalent in the industry and in accordance with industry best practices (NIST 800-53). Contractor shall maintain all appropriate administrative, physical, technical, and procedural safeguards to secure County data from data breach, protect County data and the Services from loss, corruption, unauthorized disclosure, and from hacks, and the introduction of viruses, disabling devices, malware, and other forms of malicious and inadvertent acts that can disrupt County's access and use of County data and the Services.
- b) **Contractor and the use of Email:** Contractor, including Contractor's employees and subcontractors, that are provided a County email address must only use the County email system for correspondence of County business. Contractor, including Contractor's employees and subcontractors, must not access or use personal, non-County Internet (external) email systems from County networks and/or County computing devices. If at any time Contractor's performance under this Contract requires such access or use, Contractor must submit a written request to County with justification for access or use of personal, non-County Internet (external) email systems from County networks and/or computing devices and obtain County's express prior written approval.

Contractors who are not provided with a County email address, but need to transmit County data will be required to maintain and transmit County data in accordance with this Agreement.

7. **Security Failures:** Any failure by the Contractor to meet the requirements of this Contract with respect to the security of County data, including any related backup, disaster recovery, or other policies, practices or procedures, and any breach or violation by Contractor or its subcontractors or affiliates, or their employees or agents, of any of the foregoing, shall be deemed a material breach of this Contract and may result in termination and reimbursement to County of any fees prepaid by County prorated to the date of such termination. The remedy provided in this paragraph shall not be exclusive and is in addition to any other rights and remedies provided by law or under the Contract.
8. **Security Breach Notification:** In the event Contractor becomes aware of any act, error or omission, negligence, misconduct, or security incident including unsecure or improper data disposal, theft, loss, unauthorized use and disclosure or access, that compromises or is suspected to compromise the security, availability, confidentiality, and/or integrity of County data or the physical, technical, administrative, or organizational safeguards required under this Contract that relate to the security, availability, confidentiality, and/or integrity of County data, Contractor shall, at its own expense, (1) immediately (or within 24 hours of potential or suspected breach), notify the County's Chief Information Security Officer and County Privacy Officer of such occurrence; (2) perform a root cause analysis of the actual, potential, or suspected breach; (3) provide a remediation plan that is acceptable to County within 30 days

of verified breach, to address the occurrence of the breach and prevent any further incidents; (4) conduct a forensic investigation to determine what systems, data, and information have been affected by such event; and (5) cooperate with County and any law enforcement or regulatory officials investigating such occurrence, including but not limited to making available all relevant records, forensics, investigative evidence, logs, files, data reporting, and other materials required to comply with applicable law or as otherwise required by County and/or any law enforcement or regulatory officials, and (6) perform or take any other actions required to comply with applicable law as a result of the occurrence (at the direction of County).

County shall make the final decision on notifying County officials, entities, employees, service providers, and/or the general public of such occurrence, and the implementation of the remediation plan. If notification to particular persons is required under any law or pursuant to any of County's privacy or security policies, then notifications to all persons and entities who are affected by the same event shall be considered legally required. Contractor shall reimburse County for all notification and related costs incurred by County arising out of or in connection with any such occurrence due to Contractor's acts, errors or omissions, negligence, and/or misconduct resulting in a requirement for legally required notifications.

In the case of a breach, Contractor shall provide third-party credit and identity monitoring services to each of the affected individuals for the period required to comply with applicable law, or, in the absence of any legally required monitoring services, for no less than twelve (12) months following the date of notification to such individuals.

Contractor shall indemnify, defend with counsel approved in writing by County, and hold County and County Indemnitees harmless from and against any and all claims, including reasonable attorney's fees, costs, and expenses incidental thereto, which may be suffered by, accrued against, charged to, or recoverable from County in connection with the occurrence.

Notification shall be sent to:

Andrew Alipanah, MBA, CISSP
Chief Information Security Officer
721 S. Parker St.
Suite 200
Orange, CA 92868
Phone: (714) 567-7611
Andrew.Alipanah@ocit.ocgov.com

Linda Le, CHPC, CHC, CHP
County Privacy Officer
721 S. Parker St.
Suite 200
Orange, CA 92868
Phone: (714) 834-4082
Linda.Le@ocit.ocgov.com

9. Security Audits: Contractor shall maintain complete and accurate records relating to its system and Organization Controls (SOC) Type II audits or equivalent's data protection practices, internal and external audits, and the security of any of County-hosted content, including any confidentiality, integrity, and availability operations (data hosting, backup, disaster recovery, external dependencies management, vulnerability testing, penetration testing, patching, or other related policies, practices, standards, or procedures).

Contractor shall inform County of any internal/external security audit or assessment performed on Contractor's operations, information and cyber security program, disaster recovery plan, and prevention, detection, or response protocols that are related to hosted County content, within sixty (60) calendar days of such audit or assessment. Contractor will provide a copy of the audit report to County within thirty (30) days after Contractor's receipt of request for such report(s).

Contractor shall reasonably cooperate with all County security reviews and testing, including but not limited to penetration testing of any cloud-based solution provided by Contractor to County under this Contract. Contractor shall implement any required safeguards as identified by County or by any audit of Contractor's data privacy and information/cyber security program.

In addition, County has the right to review Plans of Actions and Milestones (POA&M) for any outstanding items identified by the SOC 2 Type II report requiring remediation as it pertains to the confidentiality, integrity, and availability of County data. County reserves the right, at its sole discretion, to immediately terminate this Contract or a part thereof without limitation and without liability to County if County reasonably determines Contractor fails or has failed to meet its obligations under this section.

10. Business Continuity and Disaster Recovery (BCDR):

For the purposes of this section, "Recovery Point Objectives" means the maximum age of files (data and system configurations) that must be recovered from backup storage for normal operations to resume if a computer, system, or network goes down as a result of a hardware, program, or communications failure (establishing the data backup schedule and strategy). "Recovery Time Objectives" means the maximum duration of time and a service level within which a business process must be restored after a disaster (or disruption) in order to avoid unacceptable consequences associated with a loss of functionality.

The Contractor shall maintain a comprehensive risk management program focused on managing risks to County operations and data, including mitigation of the likelihood and impact of an adverse event occurring that would negatively affect contracted services and operations of the County. Business continuity management will enable the Contractor to identify and minimize disruptive risks and restore and recover hosted County business-critical services and/or data within the agreed terms following an adverse event or other major business disruptions. Recovery and timeframes may be impacted when events or disruptions are related to dependencies on third-parties. The County and Contractor will agree on Recovery Point Objectives and Recovery Time Objectives (as needed)) and will periodically review these objectives. Any disruption to services of system will be communicated to the County within 4 hours, and every effort shall be undertaken to restore contracted services, data, operations, security, and functionality.

All data and/or systems and technology provided by the Contractor internally and through third-party vendors shall have resiliency and redundancy capabilities to achieve high availability and data recoverability. Contractor Systems shall be designed, where practical and possible, to ensure continuity of service(s) in the event of a disruption or outage.

ATTACHMENT C

STATE PRIVACY AND SECURITY PROVISIONS

1. DEFINITIONS

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

- a. **“Assist in the Administration of the Program”** means performing administrative functions on behalf of programs, such as determining eligibility for, or enrollment in, and collecting PII for such purposes, to the extent such activities are authorized by law.
- b. **“Breach”** refers to actual loss, loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for other than authorized purposes have access or potential access to PII, whether electronic, paper, verbal, or recorded.
- c. **“Contractor Staff”** means those employees of the contractor/subcontractor, vendors and agents performing any functions for the county that require access to and/or use of PII and that are authorized by the county to access and use PII.
- d. **“PII”** is personally identifiable information that is obtained through the MEDS or IEVS on behalf of the programs and can be used alone, or in conjunction with any other reasonably available information, to identify a specific individual. The PII includes, but is not limited to, an individual's name, social security number, driver's license number, identification number, biometric records, date of birth, place of birth, or mother's maiden name. The PII may be electronic, paper, verbal, or recorded.
- e. **“Security Incident”** means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of PII, or interference with system operations in an information system which processes PII that is under the control of the county or county's Statewide Automated Welfare System (SAWS) Consortium, or CalWIN (California Welfare Information Network), or under the control of a contractor, subcontractor or vendor of the county, on behalf of the county.
- f. **“Secure Areas”** means any area where:
 - i. Contractor Staff assist in the administration of their program;
 - ii. Contractor Staff use or disclose PII; or
 - iii. PII is stored in paper or electronic format.

2. PRIVACY AND CONFIDENTIALITY

- a. The County staff, contractors, subcontractors and vendors, covered by this Agreement may use or disclose PII only as permitted in this Agreement and only to assist in the administration of programs in accordance with 45 CFR § 205.50 et. seq and Welfare and Institutions Code section 10850, and Section 14100.2 of the Welfare and Institutions Code, Section 431.300 et. Seq. of Title 42 Code of Federal Regulations, or as authorized or required by law. Disclosures, which are authorized or required by law, such as a court order, or are made with the explicit written authorization of the individual, who is the subject of the PII, are allowable. Any other use or disclosure of PII requires the express approval in writing by County of Orange. No Contractor Staff shall duplicate, disseminate or disclose PII except as allowed in this Agreement.
- b. Pursuant to this Agreement, Contractor Staff may only use PII to perform administrative functions related to administering their respective programs.
- c. Access to PII shall be restricted to Contractor Staff who need to perform their official duties to assist in the administration of their respective programs.
- d. Contractor Staff who access, disclose or use PII in a manner or for a purpose not authorized by this Agreement may be subject to civil and criminal sanctions contained in applicable federal and state statutes.

3. **PERSONNEL CONTROLS**

The County agrees to advise Contractor Staff, who have access to PII, of the confidentiality of the information, the safeguards required to protect the information, and the civil and criminal sanctions for non-compliance contained in applicable federal and state laws. For that purpose, the Contractor shall implement the following personnel controls:

- a. **Employee Training.** Train and use reasonable measures to ensure compliance with the requirements of this Agreement by Contractor Staff, including, but not limited to:
 - i. Provide initial privacy and security awareness training to each new Contractor Staff within thirty (30) days of employment and;
 - ii. Thereafter, provide annual refresher training or reminders of the privacy and security safeguards in this Agreement to all Contractor Staff. Three (3) or more security reminders per year are recommended;
 - iii. Maintain records indicating each Contractor Staff's name and the date on which the privacy and security awareness training was completed;
 - iv. Retain training records for a period of three (3) years after completion of the training.
- b. **Employee Discipline.**
 - i. Provide documented sanction policies and procedures for Contractor Staff who fail to comply with privacy policies and procedures or any provisions of these requirements.

- ii. Sanction policies and procedures shall include termination of employment when appropriate.
- c. **Confidentiality Statement.** Ensure that all Contractor Staff, accessing, using or disclosing PII, sign a confidentiality statement (provided by the County). The statement shall be signed by Contractor staff prior to accessing PII and annually thereafter. Signatures may be physical or electronic. The signed statement shall be retained for a period of three (3) years.
The statement shall include at a minimum:
 - i. General Use;
 - ii. Security and Privacy Safeguards;
 - iii. Unacceptable Use; and
 - iv. Enforcement Policies.
- d. **Background Screening.**
 - i. Conduct a background screening of a Contractor Staff before they may access PII.
 - ii. The background screening should be commensurate with the risk and magnitude of harm the employee could cause. More thorough screening shall be done for those employees who are authorized to bypass significant technical and operational security controls.
 - iii. The Contractor shall retain each Contractor Staff's background screening documentation for a period of three (3) years following conclusion of employment relationship.

4. **MANAGEMENT OVERSIGHT AND MONITORING**

To ensure compliance with the privacy and security safeguards in this Agreement the County shall perform the following:

- a. Conduct periodic privacy and security reviews of work activity by Contractor Staff, including random sampling of work product. Examples include, but are not limited to, access to case files or other activities related to the handling of PII.
- b. The periodic privacy and security reviews must be performed or overseen by management level personnel who are knowledgeable and experienced in the areas of privacy and information security in the administration of their program, and the use or disclosure of PII.

5. **INFORMATION SECURITY AND PRIVACY STAFFING**

The Contractor agrees to:

- a. Designate information security and privacy officials who are accountable for

compliance with these and all other applicable requirements stated in this Agreement.

- b. Provide County with applicable contact information for these designated individuals. Any changes to this information should be reported to County within ten (10) days.
- c. Assign staff to be responsible for administration and monitoring of all security related controls stated in this Agreement.

6. **PHYSICAL SECURITY**

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

- a. Secure all areas of the Contractor's facilities where Contractor Staff assist in the administration of their program and use, disclose, or store PII.
- b. These areas shall be restricted to only allow access to authorized individuals by using one or more of the following:
 - i. Properly coded key cards
 - ii. Authorized door keys
 - iii. Official identification
- c. Issue identification badges to Contractor Staff.
- d. Require Contractor Staff to wear these badges where PII is used, disclosed, or stored.
- e. Ensure each physical location, where PII is used, disclosed, or stored, has procedures and controls that ensure an individual who is terminated from access to the facility is promptly escorted from the facility by an authorized employee and access is revoked.
- f. Ensure there are security guards or a monitored alarm system at all times at the Contractor facilities and leased facilities where five hundred (500) or more individually identifiable records of PII is used, disclosed or stored. Video surveillance are recommended.
- g. Ensure data centers with servers, data storage devices, and/or critical network infrastructure involved in the use, storage, and/or processing of PII have perimeter security and physical access controls that limit access to only authorized Contractor Staff. Visitors to the data center area must be escorted at all times by authorized Contractor Staff.
- h. Store paper records with PII in locked spaces, such as locked file cabinets, locked file rooms, locked desks, or locked offices in facilities which have multi-use functions in one building in work areas that are not securely segregated from each other. It is

recommended that all PII be locked up when unattended at any time, not just within multi-use facilities.

- i. The Contractor shall have policies that include, based on applicable risk factors, a description of the circumstances under which the Contractor Staff can transport PII, as well as the physical security requirements during transport. A Contractor that chooses to permit its staff to leave records unattended in vehicles must include provisions in its policies to ensure the PII is stored in a non-visible area such as a trunk, that the vehicle is locked, and under no circumstances permit PII be left unattended in a vehicle overnight or for other extended periods of time.
- j. The Contractor shall have policies that indicate Contractor Staff are not to leave records with PII unattended at any time in airplanes, buses, trains, etc., including baggage areas. This should be included in training due to the nature of the risk.
- k. Use all reasonable measures to prevent non-authorized personnel and visitors from having access to, control of, or viewing PII.

7. TECHNICAL SECURITY CONTROLS

- a. **Workstation/Laptop Encryption.** All workstations and laptops, which use, store and/or process PII, must be encrypted using a FIPS 140-2 certified algorithm 128 bit or higher, such as Advanced Encryption Standard (AES). The encryption solution must be full disk. It is encouraged, when available and when feasible, that the encryption be 256 bit.
- b. **Server Security.** Servers containing unencrypted PII must have sufficient administrative, physical, and technical controls in place to protect that data, based upon a risk assessment/system security review. It is recommended to follow the guidelines documented in the latest revision of the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Security and Privacy Controls for Federal Information Systems and Organizations.
- c. **Minimum Necessary.** Only the minimum necessary amount of PII required to perform required business functions may be accessed, copied, downloaded, or exported.
- d. **Mobile Device and Removable Media.** All electronic files, which contain PII data, must be encrypted when stored on any mobile device or removable media (i.e. USB drives, CD/DVD, smartphones, tablets, backup tapes etc.). Encryption must be a FIPS 140-2 certified algorithm 128 bit or higher, such as AES. It is encouraged, when available and when feasible, that the encryption be 256 bit.
- e. **Antivirus Software.** All workstations, laptops and other systems, which process and/or store PII, must install and actively use an antivirus software solution. Antivirus software should have automatic updates for definitions scheduled at least daily.

f. **Patch Management.**

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

g. **User IDs and Password Controls.**

- i. All users must be issued a unique username for accessing PII.
- ii. Username must be promptly disabled, deleted, or the password changed upon the transfer or termination of an employee within twenty-four (24) hours. Note: Twenty-four (24) hours is defined as one (1) working day.
- iii. Passwords are not to be shared.
- iv. Passwords must be at least eight (8) characters.
- v. Passwords must be a non-dictionary word.
- vi. Passwords must not be stored in readable format on the computer or server.
- vii. Passwords must be changed every ninety (90) days or less.
- viii. Passwords must be changed if revealed or compromised.
- ix. Passwords must be composed of characters from at least three (3) of the following four (4) groups from the standard keyboard:
 - A. Upper case letters (A-Z)
 - B. Lower case letters (a-z)
 - C. Arabic numerals (0-9)
 - D. Special characters (!,@,#, etc.)

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

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

j. **Warning Banners.** The systems providing access to PII must display a warning banner stating, at a minimum:

- i. Data is confidential;
- ii. Systems are logged;
- iii. System use is for business purposes only, by authorized users; and
- iv. Users shall log off the system immediately if they do not agree with these requirements.

k. System Logging.

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

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

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

n. Intrusion Prevention. All systems involved in accessing, storing, transporting, and protecting PII, which are accessible through the Internet, must be protected by an intrusion detection and prevention solution.**8. AUDIT CONTROLS****a. System Security Review.**

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

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

- c. **Change Control.** All systems processing and/or storing PII must have a documented change control process that ensures separation of duties and protects the confidentiality, integrity and availability of data.
- d. **Anomalies.** When the County or DHCS suspects MEDS usage anomalies, the County will work with Contractor to investigate the anomalies and report conclusions of such investigations and remediation to California Department of Social Services (CDSS).

9. **BUSINESS CONTINUITY / DISASTER RECOVERY CONTROLS**

- a. **Emergency Mode Operation Plan.** The Contractor must establish a documented plan to enable continuation of critical business processes and protection of the security of PII kept in an electronic format in the event of an emergency. Emergency means any circumstance or situation that causes normal computer operations to become unavailable for use in performing the work required under this Agreement for more than twenty-four (24) hours.
- b. **Data Centers.** Data centers with servers, data storage devices, and critical network infrastructure involved in the use, storage and/or processing of PII, must include environmental protection such as cooling, power, and fire prevention, detection, and suppression.
- c. **Data Backup and Recovery Plan.**
 - i. The Contractor shall have established documented procedures to backup PII to maintain retrievable exact copies of PII.
 - ii. The documented backup procedures shall contain a schedule which includes incremental and full backups.
 - iii. The procedures shall include storing backups offsite.
 - iv. The procedures shall ensure an inventory of backup media.
 - v. The Contractor shall have established documented procedures to recover PII data.
 - vi. The documented recovery procedures shall include an estimate of the amount of time needed to restore the PII data.
 - vii. It is recommended that the Contractor periodically test the data recovery process.

10. **PAPER DOCUMENT CONTROLS**

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

- b. **Data in Vehicles.** The Contractor shall have policies that include, based on applicable risk factors, a description of the circumstances under which the Contractor Staff can transport PII, as well as the physical security requirements during transport. A Contractor that chooses to permit its staff to leave records unattended in vehicles must include provisions in its policies to ensure the PII is stored in a non-visible area such as a trunk, that the vehicle is locked, and under no circumstances permit PII be left unattended in a vehicle overnight or for other extended periods of time.
- c. **Public Modes of Transportation.** The PII in paper form shall not be left unattended at any time in airplanes, buses, trains, etc., including baggage areas. This should be included in training due to the nature of the risk.
- d. **Escorting Visitors.** Visitors to areas where PII is contained shall be escorted, and PII shall be kept out of sight while visitors are in the area.
- e. **Confidential Destruction.** PII must be disposed of through confidential means, such as cross-cut shredding or pulverizing.
- f. **Removal of Data.** The PII must not be removed from the premises of Contractor except for identified routine business purposes or with express written permission of HHS.
- g. **Faxing.**
 - i. Faxes containing PII shall not be left unattended and fax machines shall be in secure areas.
 - ii. Faxes shall contain a confidentiality statement notifying persons receiving faxes in error to destroy them and notify the sender.
 - iii. Fax numbers shall be verified with the intended recipient before sending the fax
- h. **Mailing.**
 - i. Mailings containing PII shall be sealed and secured from damage or inappropriate viewing of PII to the extent possible.
 - ii. Mailings that include five hundred (500) or more individually identifiable records containing PII in a single package shall be sent using a tracked mailing method that includes verification of delivery and receipt, unless the Contractor obtains prior written permission from HHS to use another method.

11. NOTIFICATION AND INVESTIGATION OF BREACHES AND SECURITY INCIDENTS

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

a. **Initial Notice to HHS:**

- i. The Contractor will provide initial notice to the County. The Contractor agrees to perform the following incident reporting to County.
- ii. Immediately upon discovery of a suspected security incident that involves data provided to Contractor by County, the Contractor will notify the County by email or telephone.
- iii. Within one working day of discovery, the Contractor will notify the County by email or telephone of unsecured PII, if that PII was, or is, reasonably believed to have been accessed or acquired by an unauthorized person, any suspected security incident, intrusion, or unauthorized access, use, or disclosure of PII in violation of this Agreement, or potential loss of confidential data affecting this Agreement. Notice shall be made by contacting the County as provided in this agreement, including all information known at the time.
- iv. A breach shall be treated as discovered by the Contractor as of the first day on which the breach is known, or by exercising reasonable diligence would have been known, to any person (other than the person committing the breach), who is an employee, officer or other agent of the Contractor.
- v. Upon discovery of a breach, security incident, intrusion, or unauthorized access, use, or disclosure of PII, the Contractor shall take:
 - A. Prompt corrective action to mitigate any risks or damages involved with the breach and to protect the operating environment; and
 - B. Any action pertaining to such unauthorized disclosure required by applicable Federal and State laws and regulations.

- b. **Investigation and Investigative Report.** The Contractor shall immediately investigate breaches and security incidents involving PII. The Contractor will cooperate with the County during this investigation. Within seventy-two (72) hours of discovery, the Contractor shall provide new or updated information if available to County. The updated report shall include any other applicable information related to the breach or security incident known at that time. The Contractor shall provide status update to County on a regular basis as agreed upon.

The Contractor shall provide to County all specific and pertinent information about the Breach, including copies of any reports conducted by the Contractor or on behalf of the Contractor. The Contractor shall waive any assertion of privilege in relation to such reports. Such information and/or reports shall be provided to County without unreasonable delay and in no event later than fifteen (15) calendar days the Contractor have such information and/or report.

- c. **Complete Report.** The complete report of the investigation shall include an assessment of all known factors relevant to the determination of whether a breach occurred under applicable provisions of the Health Insurance Portability and Accountability Act (HIPAA), the Health Information Technology for Economic and Clinical Health (HITECH) Act, the Information Protection Act, or other applicable law.

The report shall include a Corrective Action Plan (CAP) which includes, at a minimum, detailed information regarding the mitigation measures taken to halt and/or contain the improper use or disclosure.

If County requests additional information related to the incident, the Contractor shall make reasonable efforts to provide County with such information. County will review report and determine whether a breach occurred and whether individual notification is required. County will maintain the final decision making over a breach determination.

- d. **Notifications of Individuals.** When applicable state or federal law requires notification to individuals of a breach or unauthorized disclosure of their PII, the County will make the decision to either notify clients or have the Contractor give notice. If the Contractor shall give the notice, it would be subject to the following provisions:
 - i. If the cause of the breach is attributable to the Contractor or its subcontractors, agents or vendors, the Contractor shall pay any costs of such notifications, as well as any and all costs associated with the breach. If there are any questions as to whether the County or the Contractor is responsible for the breach, the County and the Contractor shall jointly determine responsibility for purposes of allocating the costs;
 - ii. All notifications (regardless of breach status) regarding the beneficiaries' PII shall comply with the requirements set forth in Section 1798.29 of the California Civil Code and Section 17932 of Title 42 of the United States Code, inclusive of its implementing regulations, including but not limited to the requirement that the notifications be made without reasonable delay and in no event, later than sixty (60) calendar days from discovery;
 - iii. The County has contractual requirement with the California Department of Social Services and California Department of Health Care Services to approve the time, manner and content of any such notifications and their review and approval shall be obtained before notifications are made. Therefore, the Contractor must provide the notifications to County to obtain review and approval prior to notifications are made. If notifications are distributed without State review and approval, secondary follow-up notifications may be required; and
 - iv. The County may elect to assume responsibility for such notification from the Contractor.
- e. **Responsibility for Reporting of Breaches when Required by State or Federal Law.** If the cause of a breach is attributable to the Contractor or its agents, subcontractors or vendors, the Contractor is responsible for all required reporting of the breach. If the cause of the breach is attributable to the County, the County is responsible for all required reporting of the breach. When applicable law requires the breach be reported to a federal or state agency or that notice be given to media outlets, DHCS (Department of Health Care Services) and CDSS (California Department of Social Services) (if the breach involves MEDS or SSA data), then the Contractor shall coordinate with the County to ensure such reporting is in compliance with applicable law and to prevent

duplicate reporting, and to jointly determine responsibility for purposes of allocating the costs of such reports, if any.

- f. **County Contact Information.** The Contractor shall utilize the below contact information to direct all notifications of breach and security incidents to the County. The County reserves the right to make changes to the contact information by giving written notice to the Contractor. Said changes shall not require an amendment to this Agreement or any other agreement into which it is incorporated.

Social Services Agency Contact	County Privacy Officer
County of Orange Social Services Agency Contracts Services 500 N. State College Blvd, Suite 100 Orange, CA 92868 714-541-7785 Karen.Vu@ssa.ocgov.com	Linda Le, CHC, CHPC, CHP County of Orange OCIT - Enterprise Privacy & Cybersecurity 1055 N. Main St, 6th Floor Santa Ana, CA 92701 Email: privacyofficer@ocgov.com securityadmin@ocit.ocgov.com linda.le@ocit.ocgov.com

12. **COMPLIANCE WITH SSA (SOCIAL SECURITY ADMINISTRATION) AGREEMENT**

The County has agreed to comply with applicable privacy and security requirements in the Computer Matching and Privacy Protection Act Agreement (CMPPA) between the SSA and the California Health and Human Services Agency (CHHS), in the Information Exchange Agreement (IEA) between SSA and CDSS, and in the Electronic Information Exchange Security Requirements and Procedures for State and Local Agencies Exchanging Electronic Information with SSA (TSSR). If Contractor have access to the PII data provided by SSA, then Contractor must agree to comply with the applicable privacy and security requirements, which is available upon request.

If there is any conflict between a privacy and security standard in the CMPPA, IEA or TSSR, and a standard in this Agreement, the most stringent standard shall apply. The most stringent standard means the standard which provides the greatest protection to PII.

13. COMPLIANCE WITH DEPARTMENT OF HOMELAND SECURITY AGREEMENT

The County has agreed to comply with substantive privacy and security requirements in the Computer Matching Agreement (CMA) between the Department/Agency of Homeland Security, United States Citizenship and Immigration Services (DHS-USCIS) and CDSS. If Contractor have access to the PII data provided by DHS-USCIS, then Contractor must agree to comply with the applicable privacy and security requirements, which is available upon request.

If there is any conflict between a privacy and security standard in the CMA and a standard in this Agreement, the most stringent standard shall apply. The most stringent standard means the standard which provides the greatest protection to PII.

14. CONTRACTOR AGENTS, SUBCONTRACTORS, AND VENDORS

The Contractor agrees to enter into written agreements with all agents, subcontractors, and vendors that have access to the Contractor's PII. These agreements will impose, at a minimum, the same restrictions and conditions that apply to the Contractor with respect to PII upon such agents, subcontractors, and vendors. These shall include, at a minimum, (1) restrictions on disclosure of PII, (2) conditions regarding the use of appropriate administrative, physical, and technical safeguards to protect PII, and, where relevant, (3) the requirement that any breach, security incident, intrusion, or unauthorized access, use, or disclosure of PII be reported to the Contractor. If the agents, subcontractors, and vendors of the Contractor access data provided to the County by SSA or DHS-USCIS, the Contractor shall also incorporate the Agreement's Exhibits into each subcontract or subaward with agents, subcontractors, and vendors.

15. ASSESSMENTS AND REVIEWS

In order to enforce this Agreement and ensure compliance with its provisions, the Contractor agrees to assist the County (on behalf of CDSS and DHCS) in performing compliance assessments. These assessments may involve compliance review questionnaires, and/or review of the facilities, systems, books, and records of the Contractor, with reasonable notice from the County. Such reviews shall be scheduled at times that take into account the operational and staffing demands. The Contractor agrees to promptly remedy all violations of any provision of this Agreement and certify the same to the County in writing, or to enter into a written CAP (Corrective Action Plan) with the County containing deadlines for achieving compliance with specific provisions of this Agreement.

16. ASSISTANCE IN LITIGATION OR ADMINISTRATIVE PROCEEDINGS

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



County of Orange

Information Technology Security Guidelines

ATTACHMENT D

1 ASSET MANAGEMENT

Asset management establishes an organization's inventory of fixed and controlled assets and defines how these assets are managed during their lifecycle to ensure sustained productivity in support of the organization's critical services. An event that disrupts an asset can inhibit the organization from achieving its mission. An asset management program helps identify appropriate strategies that shall allow the assets to maintain productivity during disruptive events. There are four broad categories of assets: people, information, technology, and facilities.

The Cybersecurity Program strives to achieve and maintain appropriate protection of IT assets. Loss of accountability of IT assets could result in a compromise or breach of IT systems and/or a compromise or breach of sensitive or privacy data. All vendors who contract with the County of Orange ("County") shall work cooperatively to assist County in achieving the objectives and abide by the applicable terms under these Guidelines at all times during the term of its contract with County.

1.1 GOALS AND OBJECTIVES

- 1.1.1 Services are identified and prioritized.
- 1.1.2 Assets are inventoried, and the authority and responsibility for these assets is established.
- 1.1.3 The relationship between assets and the services they support is established.
- 1.1.4 The asset inventory is managed.
- 1.1.5 Access to assets is managed.
- 1.1.6 Information assets are categorized and managed to ensure the sustainment and protection of the critical service.
- 1.1.7 Facility assets supporting the critical service are prioritized and managed.

1.2 ASSET MANAGEMENT POLICY STATEMENTS

1.2.1 Services Inventory

- 1.2.1.1 Departments shall maintain an inventory of its services. This listing shall be used by the department to assist with its risk management analysis.

1.2.2 Asset Inventory – Information

- 1.2.2.1 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 shall be used in compliance with this policy.
- 1.2.2.2 County information is a valuable asset and shall be protected from unauthorized disclosure, modification, or destruction. Prudent information security standards and practices shall 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.
- 1.2.2.3 Departments shall establish internal procedures for the secure handling and storage of all electronically maintained County information that is owned or controlled by the department.



County of Orange

Information Technology Security Guidelines

1.2.3 Asset Inventory - Technology (Devices, Software)

1.2.3.1 Departments shall maintain an inventory of all department managed devices that connect to County network resources or processes, stores, or transmits County data including but not limited to:

- Desktop computers,
- Laptop Computers,
- Tablets (iPads and Android devices),
- Mobile Phones (basic cell phones),
- Smart Phones (iPhones, Blackberry, Windows Phones and Android Phones),
- Servers,
- Storage devices,
- Network switches,
- Routers,
- Firewalls,
- Security Appliances,
- Internet of Things (IoT) devices,
- Printers,
- Scanners,
- Kiosks and Thin clients,
- Mainframe Hardware, and
- VoIP Phones.

1.2.3.2 Asset inventory shall map assets to the services they support.

1.2.3.3 Departments shall adopt a standard naming convention for devices (naming convention to be utilized as devices are serviced or purchased) that, at a minimum, includes the following:

- Department (see Appendix A for an example Department Listing)
- Facility (see Appendix B for an example Facility Listing)
- Device Type (see Appendix C for an example Device Type Listing)

1.2.3.4 Each department 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.

1.2.4 Asset Inventory - Facilities

1.2.4.1 Departments shall maintain an inventory of its facilities. This listing shall be used by the department to assist with its risk management analysis.

1.2.4.2 Departments shall identify the facilities used by its critical services.

1.2.5 Access Controls

1.2.5.1 Departments shall establish a procedure that ensures only users with legitimate business needs to access County IT resources are provided with user accounts.

1.2.5.2 Access to County information systems and information systems data shall be based on each user's access privileges. Access controls shall ensure that even legitimate users cannot access stored information unless they are authorized to do so. Access control should start by denying access to everything, and then explicitly granting access according to the "need to know" principle.

1.2.5.3 Access to County information and County information assets should be based on the principle



County of Orange

Information Technology Security Guidelines

of "least privilege," that is, grant no user greater access privileges to the information or assets than County responsibilities demand.

- 1.2.5.4 The owner of each County system, or their designee, provides written authorization for all internal and external user access.
- 1.2.5.5 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.
- 1.2.5.6 All County workforce members are to be assigned a unique user ID to access the network.
- 1.2.5.7 A user account shall 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 shall be documented prior to account creation and accounts activated only when necessary.
- 1.2.5.8 User accounts shall not be shared with others including, but not limited to, someone whose access has been denied or terminated.
- 1.2.5.9 Departments shall conduct regular reviews of the registered users' access level privileges. System owners shall provide user listings to departments for confirmation of user's access privileges.
- 1.2.6 Asset Sanitation/Disposal**
 - 1.2.6.1 Unless approved by County management, no County computer equipment shall be removed from the premises.
 - 1.2.6.2 Prior to re-deployment, storage media shall be appropriately cleansed to prevent unauthorized exposure of data.
 - 1.2.6.3 Surplus, donation, disposal or destruction of equipment containing storage media shall be appropriately disposed according to the terms of the equipment disposal services contract.
 - 1.2.6.4 Sanitization methods for media containing County information shall be in accordance with NSA standards (for example, clearing, purging, or destroying).
 - 1.2.6.5 Disposal of equipment shall be done in accordance with all applicable County, state or federal surplus property and environmental disposal laws, regulations or policies.



County of Orange

Information Technology Security Guidelines

2 CONTROLS MANAGEMENT

The Controls Management domain focuses on the processes by which an organization plans, defines, analyzes, and assesses the controls that are implemented internally. This process helps the organization ensure the controls management objectives are satisfied.

This domain focuses on the resilience controls that allow an organization to operate during a time of stress. These resilience controls are implemented in the organization at all levels and require various levels of management and staff to plan, define, analyze, and assess.

2.1 GOALS AND OBJECTIVES

- 2.1.1 Control objectives are established.
- 2.1.2 Controls are implemented.
- 2.1.3 Control designs are analyzed to ensure they satisfy control objectives.
- 2.1.4 Internal control system is assessed to ensure control objectives are met.

2.2 CONTROL MANAGEMENT POLICY STATEMENTS

2.2.1 Physical and Environmental Security

- 2.2.1.1 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.
- 2.2.1.2 Restricted areas within facilities that house sensitive or critical County information systems shall, at a minimum, utilize physical access controls designed to permit access by authorized personnel only.
- 2.2.1.3 Physical protection measures against damage from external and environmental threats shall be implemented by all departments as appropriate.
- 2.2.1.4 Access to any office, computer room, or work area that contains sensitive information shall be physically restricted from unauthorized access.
- 2.2.1.5 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.
- 2.2.1.6 Continuity of power shall be provided to maintain the availability of critical equipment and information systems.
- 2.2.1.7 Power and telecommunications cabling carrying data or supporting information services shall be protected from interception or damage. Different, yet appropriate methods shall be utilized for internal and external cabling.
- 2.2.1.8 Equipment shall be properly maintained to ensure its continued availability and integrity.
- 2.2.1.9 All shared IT infrastructure by more than one department shall meet countywide security policy for facility standards, availability, access, data & network security.



County of Orange

Information Technology Security Guidelines

2.2.2 Network Segmentation

NOTE: This section is applicable to Departments that manage their own network devices.

- 2.2.2.1 Segment (e.g., VLANs) the network into multiple, separate zones (based on trust levels of the information stored/transmitted) to provide more granular control of system access and additional intranet boundary defenses. Whenever information flows over a network of lower trust level, the information shall be encrypted.
- 2.2.2.2 Segment the network into multiple, separate zones based on the devices (servers, workstations, mobile devices, printers, etc.) connected to the network.
- 2.2.2.3 Create separate network segments (e.g., VLANs) for BYOD (bring your own device) systems or other untrusted devices.
- 2.2.2.4 The network infrastructure shall be managed across network connections that are separated from the business use of that network, relying on separate VLANs or, preferably, on entirely different physical connectivity for management sessions for network devices.

2.2.3 Mobile Computing Devices

To ensure that Mobile Computing Devices (MCDs) do not introduce threats into systems that process or store County information, departments' management shall:

- 2.2.3.1 Establish and manage a process for authorizing, issuing and tracking the use of MCDs.
- 2.2.3.2 Permit only authorized MCDs to connect to County information assets or networks that store, process, transmit, or connects to County information and information assets.
- 2.2.3.3 Implement applicable access control requirements in accordance with this policy, such as the enforcement of a system or device lockout after 15 minutes of inactivity requiring re-entering of a password to unlock.
- 2.2.3.4 Install an encryption algorithm that meets or exceeds industry recommended encryption standard for any MCD that will be used to store County information. See Section on Encryption.
- 2.2.3.5 Ensure that MCDs are configured to restrict the user from circumventing the authentication process.
- 2.2.3.6 Provide security awareness training to County employees that informs MCD users regarding MCD restrictions.
- 2.2.3.7 Label MCDs with County address and/or phone number so that the device can be returned to the County if recovered.
- 2.2.3.8 The installation of any software, executable, or other file to any County computing device is prohibited if that software, executable, or other file downloaded by, is owned by, or was purchased by an employee or contractor with his or her own funds unless approved by the department. If the device ("i" device or smartphone, only) complies with the mobile device management security standards (see section 9.2.3 Mobile Computing Devices), this is not applicable.

2.2.4 Personally Owned Devices

Personal computing devices include, but are not limited to, removable media such as thumb or USB drives, external hard drives, laptop or desktop computers, cellular phones, or personal digital assistants (PDA's) owned by or purchased by employees, contract personnel, or other non-County users.

- 2.2.4.1 The connection of any computing device not owned by the County to a County network (except the Public Wi-Fi provided for public use) or computing device is prohibited unless previously



County of Orange

Information Technology Security Guidelines

approved.

2.2.4.2 The County authorizes the use of personal devices to access resources that do not traverse the County network directly. Such resources include County's Microsoft Office 365 environment, OC Expediter, and VTI timesheet applications, to name a few. Access to some agency specific applications, e.g., applications that are subject to compliance regulations may require prior approval of the County CISO and the associated Department Head.

2.2.4.3 The County will respect the privacy of a user's voluntary use of a personally owned device to access County IT resources.

2.2.4.4 The County will only request access to the personally owned device in order to implement security controls; to respond to litigation hold (aka: e-discovery) requests arising out of administrative, civil, or criminal directives, Public Record Act requests, and subpoenas; or as otherwise required or permitted by applicable state or federal laws. Such access will be performed by an authorized technician or designee using a legitimate software process.

2.2.5 Logon Banners and Warning Notices

2.2.5.1 At the time of network login, the user shall be presented with a login banner.

2.2.5.2 All computer systems that contain or access County information shall display warning banners informing potential users of conditions of use consistent with state and federal laws.

2.2.5.3 Warning banners shall remain on the screen until the user takes explicit actions to log on to the information system.

2.2.5.4 The banner message shall be placed at the user authentication point for every computer system that contains or accesses County information. The banner message may be placed on an initial logon screen in situations where the logon provides access to multiple computer systems.

2.2.5.5 At a minimum, banner messages shall provide appropriate privacy and security information and shall contain information informing potential users that:

- User is accessing a government information system for conditions of use consistent with state and federal information security and privacy protection laws.
 - System usage may be monitored, recorded, and subject to audit.
 - Unauthorized use of the system is prohibited and subject to criminal and civil penalties.
 - Use of the system indicates consent to monitoring and recording.

2.2.6 Authentication

2.2.6.1 Authenticate user identities at initial connection to County resources.

2.2.6.2 Authentication mechanisms shall be appropriate to the sensitivity of the information contained.

2.2.6.3 Users shall not receive detailed feedback from the authenticating system on failed logon attempts.

2.2.7 Passwords

2.2.7.1 County approved password standards and/or guidelines shall be applied to access County systems. These standards extend to mobile devices (see Section 9.2.4 Mobile Computing Devices for additional guidance on mobile devices) and personally owned devices used for work (see Section 9.2.5 Personally Owned Devices for additional guidance on personally owned devices).

2.2.7.2 Passwords are a primary means to control access to systems and shall therefore be selected, used, and managed to protect against unauthorized discovery or usage. Passwords shall satisfy the following complexity rule:



County of Orange

Information Technology Security Guidelines

- Passwords will contain a minimum of one upper case letter
- Passwords will contain a minimum of one lower case letter
- Passwords will contain a minimum of one number: 1- 0
- Passwords will contain a minimum of one symbol: !, @, #, \$, %, ^, &, *, (,)
- Password characters will not be sequential (Do not use: ABCD , This is ok: ACDB)
- Passwords characters will not be repeated in a row (Do not use: P@\$\$S. This is ok: P@\$\$S\$)
- COMPLEX PASSWORD EXAMPLE: P@\$\$WoRd13

2.2.7.3 Passwords shall have a minimum length of 8 characters.

2.2.7.4 Passwords shall not be reused for twelve iterations.

2.2.7.5 Departments shall require users to change their passwords periodically (e.g., every 90 days at the maximum). Changing passwords more often than 90 days is encouraged.

2.2.7.6 Network and application systems shall be configured to enforce automatic expiration of passwords at regular intervals (e.g., every 90 days at the maximum) when the technology is feasible or available.

2.2.7.7 Newly created accounts shall be assigned a randomly generated password prior to account information being provided to the user.

2.2.7.8 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 12: Incident Management.

2.2.7.9 Users who have lost or forgotten their passwords shall 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 shall 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 shall be provided directly and only to the user in question.

2.2.7.10 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.

2.2.7.11 All passwords are to be treated as sensitive information.

2.2.7.12 User Accounts shall be locked after five consecutive invalid logon attempts within a 24-hour period. The lockout duration shall be at least 30 minutes or until a system administrator enables the user ID after investigation. These features shall be configured as indicated when the technology is feasible or available.

2.2.7.13 All systems containing sensitive information shall not allow users to have multiple concurrent sessions on the same system when the technology is feasible or available.

2.2.8 Inactivity Timeout and Restricted Connection Times

2.2.8.1 Automatic lockouts for system devices, including workstations and mobile computing devices (refer to Section 9.2.4 Mobile Computing Devices), after no more than 15 minutes of inactivity.

2.2.8.2 Automated screen lockouts shall 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 shall 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 shall not leave their computer unattended or available for someone else to use.



County of Orange

Information Technology Security Guidelines

2.2.8.3 When deemed necessary, user logins and data communications may be restricted by time and date configurations that limit when connections shall be accepted.

2.2.9 Account Monitoring

2.2.9.1 Access to a County network and its resources shall 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 shall be secured to ensure County resources are not accessed by unauthorized users.)

2.2.9.2 The control mechanisms for all types of access to County IT resources by contractors, customers or vendors are to be documented.

2.2.9.3 Monitor account usage to determine dormant accounts that have not been used for a given period, such as 45 days, notifying the user or user's manager of the dormancy.

2.2.9.4 After a longer period, such as 60 days, the account shall be disabled by the system when the technology is feasible or available.

2.2.9.5 On a periodic basis, such as quarterly or at least annually, departments shall require that managers match active employees and contractors with each account belonging to their managed staff. Security or system administrators shall then determine whether to disable accounts that are not assigned to active employees or contractors.

2.2.10 Administrative Privileges

2.2.10.1 Systems Administrators shall use separate administrative accounts, which are different from their end user account (required to have an individual end user account), to conduct system administration tasks.

2.2.10.2 Administrative accounts shall only be granted to individuals who have a job requirement to conduct systems administration tasks.

2.2.10.3 Administrative accounts shall be requested in writing and must be approved by the Department Head or designated representative (e.g., DISO) using the Security Review and Approval Process.

2.2.10.4 Systems Administrator accounts that access County enterprise-wide systems or have enterprise-wide impact shall be approved by the CISO using the Security Review and Approval Process.

2.2.10.5 Systems Administrators shall use separate administrative accounts to manage Mobile Device Management (MDM) platforms but may use the local user's credentials when configuring a mobile phone or tablet device.

2.2.10.6 All passwords for privileged system-level accounts (e.g., root, enable, OS admin, application administration accounts, etc.) shall comply with Section 9.2.8.

2.2.11 Remote Access

2.2.11.1 Departments 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.

2.2.11.2 Remote access privileges shall be granted to County workforce members only for legitimate business needs and with the specific approval of department management.



County of Orange

Information Technology Security Guidelines

- 2.2.11.3 All remote access implementations that utilize the County's trusted network environment and that have not been previously deployed within the County shall be submitted to and reviewed by OCIT Enterprise Privacy and Cybersecurity. A memorandum of understanding (MOU) shall be utilized for this submittal and review process. This is required for any Suppliers utilizing remote access to conduct maintenance.
- 2.2.11.4 Remote sessions shall be terminated after 15 minutes of inactivity requiring the user to authenticate again to access County resources.
- 2.2.11.5 All remote access infrastructures shall include the capability to monitor and record a detailed audit trail of each remote access attempt.
- 2.2.11.6 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.
- 2.2.11.7 Periodic assessments shall be performed to identify unauthorized remote connections. Results shall be used to address any vulnerabilities and prioritized according to criticality.
- 2.2.11.8 Users granted remote access to County IT infrastructure shall 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.
- 2.2.11.9 Users attempting to use external remote access shall utilize a County-approved multi-factor authentication process.
- 2.2.11.10 All remote access implementations that involve non-County infrastructures shall be reviewed and approved by both the department DISO and OCIT Enterprise Privacy and Cybersecurity. This approval shall be received prior to the start of such implementation. The approval shall be developed as a memorandum of understanding (MOU).
- 2.2.11.11 Remote access privileges to County IT resources shall not be given to contractors, customers or vendors unless department management determines that these individuals or organizations have a legitimate business need for such access. If such access is granted, it shall be limited to those privileges and conditions required for the performance of the specified work.
- 2.2.12 Wireless Access**
- 2.2.12.1 Departments 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.
- 2.2.12.2 Only wireless systems that have been evaluated for security by both department management and OCIT Enterprise Privacy and Cybersecurity shall be approved for connectivity to County networks.
- 2.2.12.3 County data that is transmitted over any wireless network shall be protected in accordance with the sensitivity of the information.
- 2.2.12.4 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.
- 2.2.12.5 Each department shall 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 shall be disabled immediately.



County of Orange

Information Technology Security Guidelines

2.2.13 System and Network Operations Management

- 2.2.13.1 Operating procedures and responsibilities for all County information processing facilities shall be formally authorized, documented, and updated.
- 2.2.13.2 Departments shall establish controls to ensure the security of the information systems networks that they operate.
- 2.2.13.3 Operational system documentation for County information systems shall be protected from unauthorized access.
- 2.2.13.4 System utilities shall be available to only those users who have a business case for accessing the specific utility.

2.2.14 System Monitoring and Logging

- 2.2.14.1 Systems operational staff shall maintain appropriate log(s) of activities, exceptions and information security events involving County information systems and services.
- 2.2.14.2 Each department shall maintain a log of all faults involving County information systems and services.
- 2.2.14.3 Logs shall be protected from unauthorized access or modifications wherever they reside.
- 2.2.14.4 The clocks of all relevant information processing systems and attributable logs shall be synchronized with an agreed upon accurate time source such as an established Network Time Protocol (NTP) service.
- 2.2.14.5 Auditing and logging of user activity shall be implemented on all critical County systems that support user access capabilities.
- 2.2.14.6 Periodic log reviews of user access and privileges shall be performed in order to monitor access of sensitive information.

2.2.15 Malware Defenses

- 2.2.15.1 Departments shall implement endpoint security on computing devices connected to the County network. Endpoint security may include one or more of the following software: anti-virus, anti-spyware, personal firewall, host-based intrusion detection (IDS), network-based intrusion detection (IDS), intrusion prevention systems (IPS), and whitelisting and blacklisting of applications, web sites, and IP addresses.
- 2.2.15.2 Special features designed to filter out malicious software contained in either email messages or email attachments shall be implemented on all County email systems.
- 2.2.15.3 Where feasible, 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 shall be verified that it is free from viruses and other forms of malicious software prior to attaining connectivity to the County network.

2.2.16 Data Loss Prevention

- 2.2.16.1 Departments shall implement host-based Data Loss Prevention (DLP) to reduce the risk of data breach related to sensitive information.
- 2.2.16.2 Departments shall deploy encryption software on mobile devices containing sensitive. See Section 9.2.19 Encryption for additional guidance.

2.2.17 Data Transfer

- 2.2.17.1 Agreements shall be implemented for the exchange of information between the County and other entities. As well as between departments.



County of Orange

Information Technology Security Guidelines

2.2.17.2 County information accessed via electronic commerce shall have security controls implemented based on the assessed risk.

2.2.18 Encryption

2.2.18.1 The decision to use cryptographic controls and/or data encryption in an application shall be based on the level of risk of unauthorized access and the sensitivity of the data that is to be protected.

2.2.18.2 The decision to use cryptographic controls and/or data encryption on a hard drive shall be based on the level of risk of unauthorized access and the sensitivity of the data that is to be protected.

2.2.18.3 Where appropriate, encryption shall be used to protect confidential (as defined by County policy) application data that is transmitted over open, untrusted networks, such as the Internet.

2.2.18.4 When cryptographic controls are used, procedures addressing the following areas shall be established by each department:

- Determination of the level of cryptographic controls
- Key management/distribution steps and responsibilities

2.2.18.5 Encryption keys shall be exchanged only using secure methods of communication.

2.2.19 System Acquisition and Development

2.2.19.1 Departments shall 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 department as well as other business applications that are used by the department but owned and/or managed by other County organizations. All business applications used by a department shall be documented in the department's IT security plan as well as their Business Impact Analysis (BIA).

2.2.19.2 An application owner shall be designated for each internal department business application.

2.2.19.3 All access controls associated with business applications shall be commensurate with the highest level of data used within the application. These same access controls shall also adhere to the policy provided in Section 7: Access Control.

2.2.19.4 Security requirements shall 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 shall be based on requirements and standards specified in this policy.

2.2.19.5 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 shall be designed and implemented to ensure that isolation.

Business Requirements

2.2.19.6 The business requirements definition phase of system development shall contain a review to ensure that the system shall adhere to County information security standards.

System Files

2.2.19.7 Operating system files, application software and data shall be secured from unauthorized use or access.

2.2.19.8 Clear-text data that results from testing shall be handled, stored, and disposed of in the same



County of Orange

Information Technology Security Guidelines

manner and using the same procedures as are used for production data.

2.2.19.9 System tests shall be performed on data that is constructed specifically for that purpose.

2.2.19.10 System testing shall not be performed on operational data unless the necessary safeguards are in place.

2.2.19.11 A combination of technical, procedural and physical safeguards shall 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.

System Development & Maintenance

2.2.19.12 The development of software for use on County information systems shall have documented change control procedures in place to ensure proper versioning and implementation.

2.2.19.13 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 shall be completed in advance in order to minimize potential security risks and disruptions to the production environment.

2.2.19.14 Any outside suppliers used for maintenance that are visitors to the facility are to be escorted and monitored while performing maintenance to critical systems. This does not apply to contractors that are assigned to work at the facility.

2.2.19.15 Systems shall be hardened, and logs monitored to ensure the avoidance of the introduction and exploitation of malicious code.

2.2.19.16 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.

2.2.19.17 In conjunction with other access control policies, any opportunity for information leakage shall be prevented through good system design practices.

2.2.19.18 Departments are responsible for managing outsourced software development related to department-owned IT systems.

System Requirements

Any system that processes or stores County Information shall:

2.2.19.19 Baseline configuration shall incorporate Principle of Least Privilege and Functionality.

2.2.19.20 Systems shall be deployed where feasible to utilize existing County authentication methods.

2.2.19.21 Session inactivity timeouts shall be implemented for all access into and from County networks.

2.2.19.22 All applications are to have access controls unless specifically designated as a public access resource.

2.2.19.23 Meet the password requirements defined in Section 9.2.8: Passwords.

2.2.19.24 Strictly control access enabling only privileged users or supervisors to override system controls or the capability of bypassing data validation or editing problems.

2.2.19.25 Monitor special privilege access, e.g., administration accounts.

2.2.19.26 Restrict authority to change master files to persons independent of the data processing function.



County of Orange

Information Technology Security Guidelines

- 2.2.19.27 Have access control mechanisms to prevent unauthorized access or changes to data, especially, the server file systems that are connected to the Internet, even behind a firewall.
- 2.2.19.28 Be capable of routinely monitoring the access to automated systems containing County Information.
- 2.2.19.29 Log all modifications to the system files.
- 2.2.19.30 Limit access to system utility programs to necessary individuals with specific designation.
- 2.2.19.31 Maintain audit logs on a device separate from the system being monitored.
- 2.2.19.32 Delete or disable all default accounts.
- 2.2.19.33 Restrict access to server file-system controls to ensure that all changes such as direct write, write access to system areas and software or service changes shall be applied only through the appropriate change control process.
- 2.2.19.34 Restrict access to server-file-system controls that allow access to other users' files.
- 2.2.19.35 Ensure that servers containing user credentials shall be physically protected, hardened and monitored to prevent inappropriate use.

2.2.20 Procurement Controls

- 2.2.20.1 Breach notification requirements clause to be included in new or renewal contracts (once policy is effective) for systems containing sensitive information.

Contractor shall report to the County within 24 hours as defined in this contract when Contractor becomes aware of any suspected data breach of Contractor's or Sub-Contractor's systems involving County's data.

- 2.2.20.2 Departments shall review all procurements and renewals for software and equipment (hosted/managed by the vendor) that transmits, stores, or processes sensitive information to ensure that vendors and contractors are aware of and are in compliance with County's cybersecurity policies if applicable. Departments shall obtain documentation supporting the business partners, contractors, consultants, or vendors compliance with County's cybersecurity policies such as:

- SOC 1 Type 2
- SOC 2 Type 2
- Security Certifications (ISO, PCI, etc.)
- Penetration Test Results

2.2.21 IT Services Provided to Public

- 2.2.21.1 Public access to County electronic information resources shall provide desired services in accordance with safeguards designed to protect County resources. All County electronic information resources are to be reviewed at least quarterly.

2.2.22 Removable Media

- 2.2.22.1 When no longer required, the contents of removable media shall be permanently destroyed or rendered unrecoverable in accordance with applicable department, County, state, or federal record disposal and/or retention requirement



County of Orange

Information Technology Security Guidelines

3 CONFIGURATION & CHANGE MANAGEMENT

Configuration and Change Management (CCM) is the process of maintaining the integrity of hardware, software, firmware, and documentation related to the configuration and change management process. CCM is a continuous process of controlling and approving changes to information or technology assets or related infrastructure that support the critical services of an organization. This process includes the addition of new assets, changes to assets, and the elimination of assets.

Cybersecurity is an integral component to information systems from the onset of the project or acquisition through implementation of:

- Application and system security
- Configuration management
- Change control procedures
- Encryption and key management
- Software maintenance, including but not limited to, upgrades, antivirus, patching and malware detection response systems

As the complexity of information systems increases, the complexity of the processes used to create these systems also increases, as does the probability of accidental errors in configuration. The impact of these errors puts data and systems that may be critical to business operations at significant risk of failure that could cause the organization to lose business, suffer damage to its reputation, or close completely. Having a CCM process to protect against these risks is vital to the overall security posture of the organization.

3.1 GOALS AND OBJECTIVES

- 3.1.1 The lifecycle of assets is managed.
- 3.1.2 The integrity of technology and information assets is managed.
- 3.1.3 Asset configuration baselines are established.

3.2 CONFIGURATION & CHANGE MANAGEMENT POLICY STATEMENTS

- 3.2.1 Changes to all information processing facilities, systems, software, or procedures shall be strictly controlled according to formal change management procedures.
- 3.2.2 Changes impacting security appliances managed by OCIT (e.g., security architecture, security appliances, County firewall, Website listings, application listings, email gateway, administrative accounts) shall be reviewed by OCIT Enterprise Privacy and Cybersecurity in accordance with the County Security Review and Approval Process.
- 3.2.3 Only authorized users shall make any changes to system and/or software configuration files.
- 3.2.4 Only authorized users shall 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 department IT management. This includes, but is not limited to, free software, computer games and peer-to-peer file sharing software.
- 3.2.5 Each department shall 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.



County of Orange

Information Technology Security Guidelines

- 3.2.6 Each department shall conduct periodic audits designed to determine if unauthorized software has been installed on any of its computers.
- 3.2.7 As appropriate, segregation of duties shall be implemented by all County departments to ensure that no single person has control of multiple critical systems and the potential for misusing that control.
- 3.2.8 Production computing environments shall be separated from development and test computing environments to reduce the risk of one environment adversely affecting another.
- 3.2.9 System capacity requirements shall be monitored, and usage projected to ensure the continual availability of adequate processing power, bandwidth, and storage.
- 3.2.10 System acceptance criteria for all new information systems and system upgrades shall be defined, documented, and utilized to minimize risk of system failure.



County of Orange

Information Technology Security Guidelines

4 VULNERABILITY MANAGEMENT

The Vulnerability Management domain focuses on the process by which organizations identify, analyze, and manage vulnerabilities in a critical service's operating environment.

4.1 GOALS AND OBJECTIVES

- 4.1.1 Preparation for vulnerability analysis and resolution activities is conducted.
- 4.1.2 A process for identifying and analyzing vulnerabilities is established and maintained.
- 4.1.3 Exposure to identified vulnerabilities is managed.
- 4.1.4 The root causes of vulnerabilities are addressed.

4.2 VULNERABILITY MANAGEMENT POLICY STATEMENTS

- 4.2.1 Departments shall develop and maintain a vulnerability management process as part of its Cybersecurity Program.



County of Orange

Information Technology Security Guidelines

5 CYBERSECURITY INCIDENT MANAGEMENT

Information Security Incident Management establishes the policy to be used by each department 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. The goal of incident management is to mitigate the impact of a disruptive event. To accomplish this goal, an organization establishes processes that:

- detect and identify events
- triage and analyze events to determine whether an incident is underway
- respond and recover from an incident
- improve the organization's capabilities for responding to a future incident

This domain defines management controls for addressing cyber incidents. The controls provide a consistent and effective approach to Cyber Incident Response aligned with Orange County's Cyber Incident Response Plan, to include:

- Collection of evidence related to the cyber incident as appropriate
- Reporting procedures including any and all statutory reporting requirements
- Incident remediation
- Minimum logging procedures
- Annual testing of the plan

5.1 GOALS AND OBJECTIVES

- 5.1.1 A process for identifying, analyzing, responding to, and learning from incidents is established.
- 5.1.2 A process for detecting, reporting, triaging, and analyzing events is established.
- 5.1.3 Incidents are declared and analyzed.
- 5.1.4 A process for responding to and recovering from incidents is established.
- 5.1.5 Post-incident lessons learned are translated into improvement strategies.

5.2 CYBERSECURITY INCIDENT MANAGEMENT POLICY STATEMENTS

- 5.2.1 Cybersecurity incident management procedures shall be established within each department to ensure quick, orderly, and effective responses to security incidents. In the event a department has not established these procedures, the department may adopt the County's Cyber Incident Response Plan. The steps involved in managing a security incident are typically categorized into six stages:
 - 5.2.2 System preparation
 - 5.2.3 Problem identification
 - 5.2.4 Problem containment
 - 5.2.5 Problem eradication
 - 5.2.6 Incident recovery
 - 5.2.7 Lessons learned
- 5.2.8 The DISO shall act as the liaison between applicable parties during a cybersecurity incident. The DISO shall be the department's primary point of contact for all IT security issues.



County of Orange

Information Technology Security Guidelines

- 5.2.9 A directory or phone tree shall be created listing all department cybersecurity incident liaison contact information.
- 5.2.10 Departments shall conduct periodic (at least annually) cybersecurity incident scenario sessions for personnel associated with the cybersecurity incident handling team to ensure that they understand current threats and risks, as well as their responsibilities in supporting the cybersecurity incident handling team.
- 5.2.11 Departments shall develop and document procedures for reporting cybersecurity incidents. For example, all employees, contractors, vendors and customers of County information systems shall be required to note and report any observed or suspected security weaknesses in systems to management. In the event a department has not established these procedures, the department may adopt the County's Cyber Incident Response Plan.
- 5.2.12 Each department shall familiarize its employees on the use of its cybersecurity incident reporting procedures.
- 5.2.13 Contact with local authorities, including law enforcement, shall be conducted through an organized, repeatable process that is both well documented and communicated.
- 5.2.14 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.
- 5.2.15 Where a follow-up action against an entity after a cybersecurity incident shall involve civil or criminal legal action, evidence shall be collected, retained, and presented to conform to the rules for evidence as demanded by the relevant jurisdiction(s). At the Department's discretion, they may obtain the services of qualified external professionals to complete these tasks.
- 5.2.16 Departments shall report cybersecurity incidents to the Central IT Service Desk in accordance with the County's Cyber Incident Reporting Policy.
- 5.2.17 Confirmed cybersecurity incidents that meet the criteria defined in the Significant Incident/Claim Reporting Protocol shall be reported by the County's Chief Information Security Officer to the Chief Information Officer (CIO), County Executive Officer (CEO), and the Board of Supervisors within 24 hours of determination that a cybersecurity incident has occurred.



County of Orange

Information Technology Security Guidelines

6 SERVICE CONTINUITY MANAGEMENT

Service continuity planning is one of the more important aspects of resilience management because it provides a process for preparing for and responding to disruptive events, whether natural or man-made. Operational disruptions may occur regularly and can scale from so small that the impact is essentially negligible to so large that they could prevent an organization from achieving its mission. Services that are most important to an organization's ability to meet its mission are considered essential and are focused on first when responding to disruptions. The process of identifying and prioritizing services and the assets that support them is foundational to service continuity.

Service continuity planning provides the organization with predefined procedures for sustaining essential operations in varying adverse conditions, from minor interruptions to large-scale incidents. For example, a power interruption or failure of an IT component may necessitate manual workaround procedures during repairs. A data center outage or loss of a business or facility housing essential services may require the organization to recover business or IT operations at an alternate location.

The process of assessing, prioritizing, planning and responding to, and improving plans to address disruptive events is known as service continuity. The goal of service continuity is to mitigate the impact of disruptive events by utilizing tested or exercised plans that facilitate predictable and consistent continuity of essential services.

This domain defines requirements to document, implement and annually test plans, including the testing of all appropriate cybersecurity provisions, to minimize impact to systems or processes from the effects of major failures of information systems or disasters via adoption and annual testing of:

- Business Continuity Plan
- Disaster Recovery Plan
- Cyber Incident Response Plan

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.

6.1 GOALS AND OBJECTIVES

- 6.1.1 Service continuity plans for high-value services are developed.
- 6.1.2 Service continuity plans are reviewed to resolve conflicts between plans.
- 6.1.3 Service continuity plans are tested to ensure they meet their stated objectives.
- 6.1.4 Service continuity plans are executed and reviewed.

6.2 SERVICE CONTINUITY MANAGEMENT POLICY STATEMENTS

- 6.2.1 Backups of all essential electronically maintained County business data shall be routinely created and properly stored to ensure prompt restoration.
- 6.2.2 Each department shall 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 department.



County of Orange

Information Technology Security Guidelines

- 6.2.3 The frequency and extent of backups shall be in accordance with the importance of the information and the acceptable risk as determined by each department.
- 6.2.4 Departments shall ensure that locations where backup media are stored are safe, secure, and protected from environmental hazards. Access to backup media shall be commensurate with the highest level of information stored and physical access controls shall meet or exceed the physical access controls of the data's source systems.
- 6.2.5 Backup media shall be labeled and handled in accordance with the highest sensitivity level of the information stored on the media.
- 6.2.6 Departments shall define and periodically test a formal procedure designed to verify the success of the backup process.
- 6.2.7 Restoration from backups shall be tested initially once the process is in place and periodically afterwards. Confirmation of business functionality after restoration shall also be tested in conjunction with the backup procedure test.
- 6.2.8 Departments shall 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 Alternate storage facilities shall be used to ensure confidentiality, integrity and availability of all County systems.
- 6.2.10 Each department shall develop, periodically update, and regularly test business continuity and disaster recovery plans in accordance with the County's Business Continuity Management Policy.
- 6.2.11 Departments shall review and update their Risk Assessments (RAs) and Business Impact Analyses (BIAs) as necessary, determined by department management (annually is recommended). As detailed in Section 14: Risk Assessment and Treatment, RAs include department 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 department has deemed critical after performing a risk analysis.
- 6.2.12 Continuity plans shall be developed and implemented to provide for continuity of business operations in the event that critical IT assets become unavailable. Plans shall provide for the availability of information at the required level and within the established Recovery Time Objective (RTO) and their location, as alternate facilities shall be used to maintain continuity.
- 6.2.13 Each department shall maintain a comprehensive plan document containing its business continuity plans. Plans shall be consistent, address information security requirements, and identify priorities for testing and maintenance. Plans shall be prepared in accordance with the standards established by the County's Business Continuity Management Policy.
Each department shall define failure prevention protocols to maintain confidentiality, integrity and availability. Departments shall automate failover procedures where applicable and maintain adequate (predictable) levels of ancillary components to meet this provision.