CONTRACT
BETWEEN
COUNTY OF ORANGE
AND
<FIRST NAME> <INITIAL> <LAST NAME>
FOR THE PROVISION OF
LICENSED AND SPECIALIZED COUNSELING PROVIDER SERVICES

This Contract is by and between the COUNTY OF ORANGE, hereinafter referred to as "COUNTY," and <FIRST NAME> <INITIAL> <LAST NAME>, licensed by the State of California, Department of Consumer Affairs, as <LICENSE>, and doing business at <STREET>, <CITY>, CA, <ZIP>, hereinafter referred to as "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 Application for Licensed and Specialized Counseling Provider Services in 2023;

WHEREAS, COUNTY desires to contract with CONTRACTOR for the provision of Licensed and Specialized Counseling Provider Services;

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

WHEREAS, such contracts are authorized and provided for pursuant to California Welfare and Institutions Code Sections 16100 and 16501;

ACCORDINGLY, THE PARTIES AGREED AS FOLLOWS:

TABLE OF CONTENTS

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

ATTACHMENT A

1. POPULATION TO BE SERVED 1
2. DEFINITIONS 1
3. HOURS OF OPERATION 3
4. SERVICE REQUIREMENTS 4
5. GOALS AND OUTCOME OBJECTIVES 12
6. REPORTING REQUIREMENTS 14
7. CLIENT RECORDS 16
8. FACILITY REQUIREMENTS 17
9. UTILIZATION REVIEW 18
10. TRAINING 18
11. COMPENSATION 19
12. CLAIMS 21
13. SERVICES DELIVERY DISPUTE RESOLUTION 22

ATTACHMENT B - COUNTY OF ORANGE INFORMATION TECHNOLOGY SECURITY PROVISIONS

EXHIBIT 1 – COUNTY OF ORANGE INFORMATION TECHNOLOGY SECURITY GUIDELINES

1. TERM

The term of this Contract shall commence on July 1, 2024, and terminate on June 30, 2027, unless earlier terminated pursuant to the provisions of Paragraph 40 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.

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 Contract 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.

3.3 CONTRATOR certifies it is in compliance with Disabled Veteran Business Enterprise requirements at the time this Contract is executed.

4. DESCRIPTION OF SERVICES

4.1 CONTRACTOR agrees to provide those services, facilities, equipment, and supplies, as described in Attachment A to the Contract between County of Orange and <FIRST NAME> <INITIAL> <LAST NAME>, for the Provision of Licensed and Specialized Counseling Provider Services, attached hereto and incorporated herein by reference.

4.2 Upon the request of ADMINISTRATOR, CONTRACTOR shall 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 24 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.

6. DELEGATION AND ASSIGNMENT

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.

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.

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

<u>County Civil Rights Contact</u>:

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: [Contractor's Name]
[Mailing Address]
[City, State, Zip Code]

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 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.

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

13.4 Qualified Insurer

13.4.1 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).

13.4.2 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.

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

Coverage	Minimum Limits
Commercial General Liability	$1,000,000 per occurrence $2,000,000 aggregate
Workers' Compensation (*)	Statutory
Employer's Liability Insurance (*)	$1,000,000 per accident or disease
Network Security & Privacy Liability	$25,000 per claims-made
Professional Liability Insurance	$1,000,000 per claims made $1,000,000 aggregate
Sexual Misconduct Liability (*)	$1,000,000 per occurrence

(*) Workers' Compensation, and Employer's Liability Insurance will not be required by this Contract of any CONTRACTOR without employees.

13.5 Required Coverage Forms

13.5.1 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 Required Endorsements

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

13.6.1.1 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.

13.6.1.2 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.

13.6.2 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 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.

13.8 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.

13.9 If CONTRACTOR's Professional Liability, and Network Security & Privacy Liability policy are a "Claims-Made" policy, CONTRACTOR shall agree to the following:

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

13.9.2 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.

13.9.3 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.

13.10 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).

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

13.12 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.

13.13 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.

13.14 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.

13.15 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 funds intended for the purposes of this Contract with any funds made available under this Contract. CONTRACTOR shall not claim payment 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. BREACH SANCTIONS

18.1 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:

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

18.1.2 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

18.1.3 Offset against any monies billed by CONTRACTOR but yet unpaid by COUNTY those monies disallowed pursuant to Subparagraph 18.1.2 above.

18.2 ADMINISTRATOR will give CONTRACTOR written notice of any action

pursuant to this Paragraph, which notice shall be deemed served on the date of mailing.

19. PAYMENTS

19.1 Allowable Costs and Usage

During the term of this Contract, COUNTY shall pay CONTRACTOR monthly in arrears, one-hundred and twenty dollars ($120) per counseling hour for each referral, subject to any exclusions or limitations specified in Attachment A. No guarantee is given by COUNTY to CONTRACTOR regarding usage of this Contract. CONTRACTOR agrees to supply the services at the unit price listed above, regardless of the number of referrals from COUNTY.

19.2 Claims

19.2.1 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 19.2.4. 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.

19.2.2 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 23 of this Contract.

19.2.3 Payments should be released by COUNTY within a reasonable time

period of approximately thirty (30) days after receipt of a correctly completed claim form and required supporting documentation.

19.2.4 Year-End and Final Claims

19.2.4.1 During each COUNTY fiscal year, July 1 through June 30, covered under the term of this Contract, COUNTY may establish two (2) billing periods (June 1st through June 15th and June 16th through June 30th) for the month of June which shall require CONTRACTOR submit separate invoice claims for each billing period. In the event COUNTY determines a need for two (2) billing periods during any or all COUNTY fiscal years, COUNTY will provide written notification to CONTRACTOR by the 15th of May of each corresponding fiscal year, which will inform CONTRACTOR of applicable invoice claim deadlines.

19.2.4.2 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.

19.2.4.3 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.

20. 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.

21. 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.

22. REVENUE

22.1 Whenever CONTRACTOR receives any money specifically designated for use in programs funded through this Contract, such monies shall be considered to be a cost off-set and treated as a reduction against the amount claimed by CONTRACTOR.

22.2 CONTRACTOR is not required to apply grants or gifts which are unrestricted in use to any cost or expense of CONTRACTOR in which COUNTY participates.

22.3 CONTRACTOR may establish and utilize a sliding fee schedule, approved by ADMINISTRATOR, to determine client fees for services provided. However, CONTRACTOR shall not refuse services to clients referred by

ADMINISTRATOR because of inability or unwillingness to pay said fees.

22.4 CONTRACTOR shall make every reasonable effort to collect all available third party reimbursement for which client may be eligible. Public and private insurance carriers shall be billed on the basis of CONTRACTOR's customary charges, if applicable.

22.5 Fees and revenues received by CONTRACTOR from or on behalf of clients, including from public or private insurance carriers, shall be deducted from any billings to COUNTY and shall reduce any obligation of COUNTY under this Contract.

23. RECORDS, INSPECTIONS, AND AUDITS

23.1 Financial Records

23.1.1 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.

23.1.2 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.

23.2 Client Records

23.2.1 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.

23.2.2 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 40.2 of this contract.

23.2.3 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.

23.3 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.

23.4 Inspections and Audits

23.4.1 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.

23.4.2 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.

23.4.3 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.

23.4.4 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.

23.5 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.

24. PERSONNEL DISCLOSURE

24.1 This Paragraph 24 applies to all of CONTRACTOR's personnel providing services through this Contract, paid and unpaid, who have contact with clients served through this Contract (hereinafter referred to as "Personnel").

24.2 CONTRACTOR shall make available to ADMINISTRATOR a current list of all Personnel, upon request. Personnel records could include, but are not limited to, résumés and job applications.

24.3 Where authorized by law, CONTRACTOR shall disclose to ADMINISTRATOR if CONTRACTOR and any of CONTRATOR's Personnel who have criminal convictions or has been the subject of a child abuse investigation.

24.4 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).

24.5 In the event a record is revealed through the process described in above Subparagraph 24.4, or a disclosure of criminal convictions or child abuse investigations, COUNTY will be available to consult with CONTRACTOR on appropriateness of CONTRACTOR's Personnel's interaction with clients receiving services through this Contract.

24.6 CONTRACTOR warrants that all Personnel have satisfactory and appropriate backgrounds to perform duties related to clients receiving services through this Contract.

24.7 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 have contact with clients 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 18 above.

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

24.9 Disqualification, if any, of CONTRACTOR Personnel, pursuant to this Paragraph 24 shall not relieve CONTRACTOR of its obligation to complete all work in accordance with the terms and conditions of this Contract.

25. 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.

26. EDD INDEPENDENT CONTRACTOR REPORTING REQUIREMENTS

26.1 Effective January 1, 2001, COUNTY is required to file Federal Form 1099-Misc for services received from a "service provider" to whom COUNTY pays $600 or more or with whom COUNTY enters into a contract for $600 or more within a single calendar year. The purpose of this reporting requirement is to increase child support collection by helping to locate parents who are delinquent in their child support obligations.

26.2 The term "service provider" is defined in California Unemployment Insurance Code Section 1088.8, Subparagraph (b)(2) as, "An individual who is not an employee of the service recipient for California purposes and who received compensation or executes a contract for services performed for that service recipient within or without the state." The term is further defined by the California Employment Development Department to refer specifically to independent contractors. An independent contractor is defined as, "An individual who is not an employee of the ... government entity for California purposes and who receives compensation or executes a contract for services performed for that ... government entity either in or outside of California."

26.3 The reporting requirement does not apply to corporations, general partnerships, limited liability partnerships, and limited liability companies.

26.4 Additional information on this reporting requirement can be found at the California Employment Development Department web site located at

https://edd.ca.gov/Payroll_Taxes/Independent_Contractor_Reporting.htm. To comply with the reporting requirements, COUNTY procedure for contracting with independent contractors mandates that the following information be completed and forwarded to ADMINISTRATOR immediately upon request:

26.4.1 First name, middle initial, and last name;

26.4.2 Social Security number;

26.4.3 Address;

26.4.4 Start and expiration dates of contract; and

26.4.5 Amount of contract.

26.5 The failure of CONTRACTOR to timely submit the requested data shall constitute a material breach and grounds for termination of this Contract.

27. 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.

28. 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.

29. CONFIDENTIALITY

29.1 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.

29.2 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 Contract 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.

29.3 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.

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

29.5 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.

29.5.1 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.

29.5.2 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.

30. SECURITY

CONTRACTOR shall abide by the requirements in Attachment B attached hereto and incorporated by reference.

31. COPYRIGHT ACCESS

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

32. WAIVER

No delay or omission by either party hereto to exercise any right or power accruing upon any noncompliance or default by the other party with respect to any of the terms of this 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 Contracts 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 Contract herein contained.

33. SERVICES DURING EMERGENCY AND/OR DISASTER

33.1 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.

33.2 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.

33.3 CONTRACTOR shall service COUNTY during emergencies and/or declared disaster under the same terms and conditions that apply during non-emergency/disaster conditions**.** Compensation of services provided during or after an emergency/disaster shall be calculated by the same unit 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.

33.4 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.

34. PUBLICITY, LITERATURE, ADVERTISEMENTS AND SOCIAL MEDIA

34.1 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.

34.2 CONTRACTOR may develop and publish information related to this Contract where all of the following conditions are satisfied:

34.2.1 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;

34.2.2 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;

34.2.3 The information does not give the appearance that the COUNTY, its officers, employees, or agencies endorse:

34.2.3.1 Any commercial product or service; and

34.2.3.2 Any product or service provided by CONTRACTOR, unless approved in writing by ADMINISTRATOR; and

34.2.4 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.

35. REPORTS

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

35.2 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.

36. 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).

37. 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:

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

37.2 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

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

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

38.1 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 38.1.1 - 38.1.1.4.

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

38.1.1.1 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.

38.1.1.2 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.

38.1.1.3 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.

38.1.1.4 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.

39. 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.

40. TERMINATION PROVISIONS

40.1 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.

40.2 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.

40.3 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.

40.4 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.

40.5 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.

41. COOPERATIVE CONTRACT

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

41.2 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 Contracts, providing for their own acceptance, and making any subsequent payments. Contractor shall be required to include in any Contract 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 Contract 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 Contract. 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.

41.3 As a cost-recovery mechanism for County, a 2 percent administrative rebate on total sales from all subordinate contracts will be paid to the County for any contracts

the Contractor agrees to enter into with another agency or entity, other than the County of Orange or a department thereof, under the provisions and pricing of this Contract. The County has partnered with Pavilion, a third-party administrator, responsible for managing all reporting and payments under this Cooperative Program. The Contractor shall provide quarterly Volume Sales Reports about additional sales to other entities under the provisions and pricing of this Contract. The Reports shall include the ordering agency, detail of items sold including description, quantity, and price, and shall include all transactions pertaining to sales under the Contract provisions and pricing for that Reporting Period. Contractor shall provide the Volume Sales Reports regardless of whether or not any sales have been conducted. Failure of the Contractor to provide quarterly reports as required may be deemed by the County as a material breach of the Contract. A late penalty of 15 percent on the value of the rebate may be assessed to the Contractor for each month the payments are not received.

41.4 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.

42. 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.

43. SIGNATURE IN COUNTERPARTS

43.1 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.

43.2 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: ***NAME OF PROVIDER***

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 S. Frost Print Name	Deputy County Counsel Title
DocuSigned by: Carolyn S. Frost D3AB98D76D0B425... Signature	4/19/2024 | 1:59:22 PM PDT Date

ATTACHMENT A

SCOPE OF WORK

FOR THE PROVISION OF

LICENSED AND SPECIALIZED COUNSELING PROVIDER SERVICES

1. POPULATION TO BE SERVED

CONTRACTOR shall provide services to clients referred by Social Services Agency (SSA). Clients include children ages birth through seventeen (17) years of age, and non-minor dependents, who are at risk of, or have a history of child abuse and/or neglect, and parents and/or caregivers. At the time of referral, some clients are in crisis and may require immediate intervention services and/or resources, and/or may be in jeopardy of having children placed out of the home. Other clients may have had their children removed from the home and require intervention services and/or resources to assist them in reunifying with their children under a time-limited case plan with the Orange County Juvenile Court. Population to be served shall hereafter be referred to as "CLIENTS."

2. DEFINITIONS

2.1 Abuse: Refers to various types of abuse, including, but not limited to, physical, sexual, general neglect, and emotional abuse.

2.2 Assigned Social Worker (ASW): County of Orange Social Worker responsible for CLIENT(s) case management.

2.3 Authorization Number: The written number designated by Resource Development and Management (RDM) per referral, located on the original date-stamped Client Referral form.

2.4 Case Notes: A written record of documented activities performed and signed by CONTRACTOR maintained in the CLIENT's case file.

2.5 Child and Family Team (CFT) Meeting: A family-centered, strength-based, collaborative process to develop a plan of care, placement changes, and service needs for the child, youth/young adult, or NMD in out-of-home care.

2.6 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.

2.7 Danger Statements: Detailed, short, behaviorally-based statements using non-judgmental language describing specific worries for the future safety of children while with their caregiver, which describe the potential caregiver's behavior and the potential future impact on the child.

2.8 Harm Statements: Detailed, short, behaviorally-based statements using non-judgmental language describing past actions/inaction by the caregiver that have hurt the child either physically, sexually, developmentally, or emotionally, which describe the caregiver's behavior and the impact on the child.

2.9 Network of Support/Family Connections: A group comprised of family members, friends, community, child welfare, and other professionals that comes together to support a family in keeping the child safe. Members of the network are part of a family's support system for long-term care.

2.10 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 the Juvenile Court, up to twenty-one (21) years of age.

2.11 Resource Development and Management (RDM): A unit of staff within the Children and Family Services (CFS) Division who coordinate referrals for services and authorize/terminate contracted services at the request of CLIENTS' ASW.

2.12 Safety Goal: Detailed, short, behaviorally-based statements using non-judgmental language and describing specific actions the parents and network will demonstrate to create and sustain child safety.

2.13 Safety Organized Practice (SOP): A holistic approach to collaborative teamwork in

child welfare that seeks to build and strengthen partnerships within a family, their informal support network of friends and family, and the agency. SOP utilizes strategies and techniques in line with the belief that a child and his or her family are the central focus and that the partnership exists in an effort to find solutions that ensure safety, permanency, and well-being for children.

2.14 Social and Family History: A written statement documenting social and family history relevant to reasons for referral, and include a mental status exam, substance abuse, and domestic violence evaluations.

2.15 Telehealth Counseling Services: Counseling services which must be conducted subject to the State of California Board of Behavioral Sciences (BBS) Standards of Practice statues and regulations for Telehealth, and in compliance with the Business and Professions Code 2290.5.

2.16 Therapeutic Monitored Observation (TMO): Consists of CONTRACTOR observing Client(s) in a specific setting or environment in order to identify specific treatment needs at a location other than CONTRACTOR's office and may occur in addition to, or in lieu of the weekly counseling session.

3. HOURS OF OPERATION

3.1 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 services Monday through Friday, from 8:00 a.m. to 5:00 p.m., except COUNTY holidays as established by the Orange County Board of Supervisors. However, CONTRACTOR is encouraged to provide the contracted services on holidays, whenever possible.

3.2 CONTRACTOR shall also be available to provide counseling services during evening hours, between 5:00 p.m. to 8:00 p.m., a minimum of three (3) days per week, Monday through Friday.

3.3 CONTRACTOR may substitute up to three (3) hours on Saturday or Sunday for the same number of evening hours provided in the evening, on Monday through

Friday.

3.4 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 3.1 of this Attachment A. Any unauthorized closure shall be deemed a material breach of this Contract, pursuant to Paragraph 18, and shall not be reimbursed.

4. SERVICE REQUIREMENTS

All services provided require written pre-authorization in the form of a referral by the CFS RDM program prior to any services being rendered.

4.1 CONTRACTOR's services shall address, as identified by ASW and/or Juvenile Court, areas of intervention, including, but not limited to, physical abuse, general neglect, emotional abuse, domestic violence, sexual abuse, substance abuse, and mental health issues.

4.2 CONTRACTOR shall provide services that meet the needs of CLIENTS who may lack coping skills, communication skills, and the skills and/or resources necessary to provide a safe environment for their children. Services shall address common problems that include, but are not limited to, inadequate housing, poor nutrition, and lack of basic needs (e.g., food, beds, utilities, etc.).

4.3 CONTRACTOR shall deliver culturally responsive services to CLIENTS as described in Subparagraph 2.6.

4.4 CONTRACTOR shall integrate the Safety Organized Practice strategies and techniques, as defined in Subparagraph 2.13, into services provided.

CONTRACTOR shall provide the following services:

4.5 Intake Assessment

CONTRACTOR shall conduct an Intake Assessment, in a collaborative manner

with CLIENTS, which includes clinical evaluation and assessment of social family history, mental status exam, substance abuse, domestic violence, Danger Statements defined in Subparagraph 2.7, Harm Statements defined in Subparagraph 2.8, Safety Goal defined in Subparagraph 2.12, and Network of Support/Family Connections defined in Subparagraph 2.9. If domestic violence, suicidal ideation, or substance abuse are identified, CONTRACTOR shall develop a safety plan with CLIENT to address any immediate and/or ongoing safety concerns.

4.5.1 CONTRACTOR shall also identify behaviors and problems defined in the Diagnostic and Statistical Manual of Mental Disorders, Fifth Edition (DSM-5), which could endanger or place child(ren) at risk of abuse and/or neglect.

4.5.1.1 CONTRACTOR shall determine appropriate treatment plan for identified DSM-5 behaviors.

4.5.2 CONTRACTOR shall develop a treatment plan from the Intake Assessment, as described in Subparagraphs 4.5 through 4.5.1.1, and ensure the plan includes and is aligned with CLIENT treatment goals in the resulting Assessment and Treatment Plan (ATP) described in Subparagraph 6.1.

4.5.3 CONTRACTOR may use a maximum of up to three (3), fifty (50) minute sessions per CLIENT to complete the Intake Assessment.

4.5.4 The initial pre-authorized five (5) month service period begins with the date of the first Intake Assessment interview and ends five (5) months later.

4.5.5 CONTRACTOR shall begin the Intake Assessment within thirty (30) days of the referral stamp date and shall ensure the resulting ATP is received by ADMINISTRATOR within sixty (60) calendar days of the referral stamp date. If ADMINISTRATOR does not receive the ATP within sixty (60) calendar days of the referral stamp date, the Authorization Number as defined in Subparagraph 2.3 will no longer be valid and CONTRACTOR shall not be compensated for any services provided under said Authorization Number.

4.6 Counseling Services

4.6.1 CONTRACTOR shall provide pre-authorized counseling services at one (1) counseling hour per week, for twenty (20) consecutive weeks, over the five (5) month authorization period.

4.6.2 Each counseling hour shall consist of fifty (50) minutes of direct counseling services and ten (10) minutes of case administration.

4.6.3 As directed by ASW, CONTRACTOR shall provide individual, conjoint, and/or family counseling services in any combination to assist CLIENTS to identify and understand problems related to child abuse and/or neglect, including, but not limited to, substance abuse and domestic violence, and to achieve counseling goals and modify behavior.

4.6.3.1 Individual counseling means one (1) CLIENT (may refer to a child or adult) specified on the referral form.

4.6.3.2 Conjoint counseling means two (2) CLIENTS, not the child, listed on the referral form.

4.6.3.3 Family counseling means at least one (1) parent/caregiver and at least one (1) child listed on the referral form.

4.6.3.4 Face-to-face contact is the first and primary choice for conducting counseling services with CLIENTS.

4.6.3.5 On a case-by-case basis, CONTRACTOR may provide Telehealth Counseling Services as defined in Subparagraph 2.15 of this Attachment A as an alternative to face-to-face contact and only with written pre-authorization from RDM and concurrence from ASW.

4.6.4 CONTRACTOR shall provide no more than one (1) counseling hour per calendar week, per Authorization Number, beginning with the authorization start date, and ending no later than the authorization end date. CONTRACTOR shall submit a written request for any exceptions, in advance, to RDM.

4.6.4.1 The authorization start date means the referral stamp date which is provided by RDM and noted on the referral form.

4.6.4.2 The authorization end date means five (5) months of services from the first Intake Assessment session.

4.6.4.3 The calendar week is defined as Monday through Sunday.

4.6.4.4 Written pre-authorization from RDM is required for any extended counseling sessions after the initial authorization end date.

4.6.5 CONTRACTOR shall conduct no more than six (6) counseling hours per day for CLIENTS. Payment shall not be authorized for more than six (6) counseling hours per day, except in certain circumstances that are discussed in advance with ASW and pre-authorized by RDM.

4.6.6 Should CONTRACTOR and/or ASW determine that additional individuals need to be served under an existing referral, CONTRACTOR shall obtain written pre-authorization from RDM before these additional individuals may receive services. These additional individuals shall be referred to as Add-On CLIENTS. Verbal approval by ASW does not designate pre-authorization. Compensation will only be paid to CONTRACTOR for pre-authorized Add-On CLIENTS.

4.7 Extension Request

CONTRACTOR shall make every effort to achieve treatment goals within the five (5) month service period. To extend services, CONTRACTOR must submit an Extension Request ATP to RDM at least thirty (30) days in advance of termination date of the original service period. CONTRACTOR must receive written pre-authorization before extending services.

4.8 Crisis Session

CONTRACTOR may conduct a crisis session for an authorized CLIENT which consists of an unscheduled emergency session to assess and/or protect a CLIENT's health and/or safety.

4.8.1 CONTRACTOR shall provide written justification to RDM within one (1) business day and notify ASW of CLIENT's crisis session. Crisis sessions cannot be ongoing in lieu of regularly scheduled appointments.

4.9 Extenuating Circumstances Session

CONTRACTOR may conduct an additional counseling hour to a CLIENT in addition to the regular weekly counseling hour, with written pre-authorization from RDM when a CLIENT requires additional service on a temporary basis, as determined by ASW, and/or in clinical consultation with CONTRACTOR.

4.10 Community Resource Linkage

4.10.1 CONTRACTOR shall assess CLIENT-specific needs on an ongoing basis and shall provide referrals to appropriate community resources, such as Family Resource Centers, throughout the course of services, and upon termination of services. CONTRACTOR shall follow-up with CLIENTS on the status of referrals provided.

4.10.2 CONTRACTOR shall clearly document on the ATP, Case Notes, and Termination Report the community resource linkages provided to CLIENT and the status of CLIENTS' utilization of such linkages.

4.11 Exceptions to any of the services described in Paragraph 4 of this Attachment A must have written pre-authorization from RDM.

4.12 Court Letters

CONTRACTOR shall prepare letters for the purpose of informing the Orange County Juvenile Court of the status of CLIENT's progress, if requested, with written pre-authorization from RDM. The requested content of a court letter may vary and shall be determined by ASW and/or Orange County Juvenile Court.

4.13 CFT Meetings or TMOs

CONTRACTOR shall participate in CFT Meetings defined in Subparagraph 2.5 or TMOs defined in Subparagraph 2.16, at the request of ASW with written pre-authorization from RDM.

4.14 Juvenile Court Testimony

CONTRACTOR shall appear in Juvenile Court prepared to testify, and/or to produce pertinent case records on matters regarding CLIENTS served, when requested by SSA.

4.15 No Show (NS) Policy

CONTRACTOR shall comply with the following:

4.15.1 A missed appointment is considered a NS unless CLIENT contacts CONTRACTOR at least twenty-four (24) hours in advance of a scheduled appointment to reschedule within the same calendar week (Monday to Sunday). CONTRACTOR shall telephonically inform ASW of each NS within twenty-four (24) hours.

4.15.2 CONTRACTOR shall notify CLIENT and ASW by written NS letter in the appropriate primary language on a form provided by ADMINISTRATOR, within forty-eight (48) hours, each time CLIENT has a NS.

4.15.3 If one (1) of the CLIENTS on a multiple-CLIENT referral is a NS more than once, CONTRACTOR may serve the remaining CLIENTS and contact ASW to review status of the referral.

4.15.4 CONTRACTOR shall suspend services if CLIENT(s) accumulate(s) three (3) NS's and shall notify ASW by telephone within twenty-four (24) hours, and by written letter within forty-eight (48) hours, and inquire whether CLIENT(s) should be reinstated.

4.16 Reinstatement Policy

CONTRACTOR shall comply with the following:

4.16.1 ASW may reinstate CLIENT(s) for services within ten (10) calendar days of receipt of the third NS letter from CONTRACTOR. A CLIENT may be reinstated only once during the service period; however, exceptions may be made by ASW for a CLIENT with a court-ordered case plan. In such cases, CONTRACTOR shall schedule the reinstated CLIENT in the next available service slot. If ASW does not reinstate CLIENT within (10) calendar days, CONTRACTOR shall terminate referral.

4.17 Financial Assessment

CONTRACTOR shall conduct a Financial Assessment with adult CLIENTS using a sliding fee schedule provided by ADMINISTRATOR, to determine fees for services that adult CLIENTS may be able to pay, for services received. However,

CONTRACTOR shall not refuse services to CLIENTS referred by ADMINISTRATOR because of inability or unwillingness to pay.

4.18 Receipt for Services (RFS)

CONTRACTOR shall require an RFS form to be signed and dated by all adult CLIENTS receiving services on the day services are received.

4.18.1 CONTRACTOR shall have the parent/caregiver or other responsible adult present sign and date the RFS form on behalf of minors receiving services. If an unaccompanied minor receives services, CONTRACTOR shall notify ASW and document such on RFS form and CONTRACTOR case notes.

4.18.2 CONTRACTOR shall document fees collected from CLIENTS, public and private insurance carriers, and, including, but not limited to, Medi-Cal reimbursement for services provided on the RFS form.

4.19 Client Engagement

CONTRACTOR shall develop a plan to actively engage CLIENTS that are unresponsive or difficult to engage in counseling services, to facilitate achievement of the goals and outcome objectives described in Paragraph 5 of this Attachment A.

4.20 Special Incident Report

If a CLIENT displays unusual, aggressive, or high-risk behavior or there are any injuries during service delivery, CONTRACTOR shall notify ASW or the CFS Officer of the Day as designated on ASW's voice message immediately by telephone, and submit a written Special Incident Report (SIR) to ADMINISTRATOR within twenty-four (24) hours on a form provided by ADMINISTRATOR.

4.21 Documentation Standards

CONTRACTOR shall ensure all documentation will be type-written, including, but not limited to, the following:

4.21.1 Original and Revised ATPs;

4.21.2 Termination Reports;

4.21.3 Case notes;

4.21.4 Telephonic consultation with CLIENT(S), CFS staff and/or authorized collateral contacts;

4.21.5 Monthly telephonic contact and progress reports with ASW; and

4.21.6 Receipt for Services, invoices, and claim forms.

4.22 CONTRACTOR shall not provide transportation to any SSA CLIENTS.

4.23 CONTRACTOR shall be available to accept a minimum of one (1) referral per month.

4.24 CONTRACTOR shall attempt to reschedule CLIENT sessions in the same week should CONTRACTOR become unavailable to provide services for a regular scheduled session, and document attempted efforts.

4.25 CONTRACTOR shall notify all CLIENTS and ADMINISTRATOR at least one (1) week in advance of scheduled leave that will exceed one (1) week (e.g., vacations, medical leave). To ensure CLIENTS are aware of resources during CONTRACTOR's absence, CONTRACTOR shall record a voicemail greeting at the phone number CLIENTS normally call which shall indicate the scheduled date of return and provide telephone number(s) for emergency assistance and mental health emergencies.

4.26 CONTRACTOR shall submit written notification to ADMINISTRATOR if counseling services are provided to a CLIENT after termination of the authorized contract service period.

4.27 CONTRACTOR shall not allow any other person, (e.g., intern, volunteer, employee, colleague, etc.,) to provide counseling services or documentation related to services to CLIENTS on behalf of CONTRACTOR.

4.28 CONTRACTOR shall not conduct counseling services under any separate contracts with any CLIENT during the contract service period.

4.29 CONTRACTOR's employment aside from this counseling services contract shall not interfere with or cause disruption to services provided under this Contract.

4.30 CONTRACTOR shall immediately provide written notification to

ADMINISTRATOR of any change in status to CONTRACTOR's valid and current professional license and/or if CONTRACTOR becomes subject to any form of disciplinary action initiated by the BBS, or Board of Psychology (BOP), during the term of this Contract.

4.31 Notwithstanding anything to the contrary, it is mutually understood that CONTRACTOR may request to be placed on voluntary hold from receiving referrals due to conflicts in schedule, caseload size limitations, etc. Should CONTRACTOR request to be placed on a voluntary hold, CONTRACTOR shall submit a written request to SSA.

4.32 Notwithstanding anything to the contrary, it is mutually understood that CONTRACTOR may be placed on administrative hold by SSA, based on the needs of, and at the sole discretion of the COUNTY.

4.33 In the event CONTRACTOR is no longer able to conduct counseling services under this Contract, CONTRACTOR shall submit a written request to SSA and include an explanation as to why CONTRACTOR cannot continue to provide counseling services.

5. GOALS AND OUTCOME OBJECTIVES

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 its outcomes and evaluation. Developed by the Center for Social Policy, the Strengthening Families Model identifies Five (5) Protective Factors, described below, that have been identified in preventing the risk of child abuse and neglect.

5.1 CONTRACTOR shall incorporate the following Five (5) Protective Factors into counseling services provided to SSA CLIENTS:

5.1.1 Social Connections: Isolated families lead to a higher risk of child abuse. Families need to build trusting relationships and connect with others to strengthen parenting skills and decrease risk of abuse.

5.1.2 Knowledge of Parenting and Child Development: This leads to appropriate expectations and the use of more developmentally appropriate

guidance techniques.

5.1.3 Social and Emotional Competence of Children: Children who are educated about identifying feelings, empathizing with others, sharing emotions appropriately, and problem-solving, have more positive interactions with others.

5.1.4 Concrete Support in Times of Need: Immediate support and resources should be provided when a family is in crisis.

5.1.5 Parental Resilience: This involves bouncing back from difficulties, i.e., recognizing challenges/feelings in difficult times, and the ability to have hope, problem-solve, and take action.

5.2 ADMINISTRATOR will supply CONTRACTOR with the Protective Factors Evaluation Tool (and/or other SSA approved evaluation tools) to help determine how counseling services are impacting SSA CLIENTS to facilitate outcome measures.

5.3 Pre-Tests and Post-Tests

5.3.1 CONTRACTOR shall conduct pre-tests and post-tests provided by ADMINISTRATOR, to assess and measure change in CLIENT(s) progress.

5.3.1.1 CONTRACTOR shall conduct the pre-test during the Intake Assessment, and shall attach the completed pre-test to the ATP, which is due within sixty (60) calendar days of the referral stamp date.

5.3.2 CONTRACTOR shall conduct the post-test during the Termination session and attach the completed post-test to the Termination Report, which is due within fifteen (15) calendar days of service termination and/or upon request of ADMINISTRATOR.

5.4 Goals

5.4.1 CONTRACTOR understands and agrees that the primary goal for Counseling Services is to assist CLIENTS at risk or with a history of abuse and/or neglect to strengthen their relationships and support successful

family maintenance and/or reunification.

5.5 Performance Outcome Objectives

CONTRACTOR shall meet the following outcome objectives during each fiscal year of this Contract:

5.5.1 A minimum of seventy percent (70%) of CLIENTS who begin counseling services will complete services.

5.5.2 A minimum of eighty percent (80%) of CLIENTS who complete counseling services will demonstrate improvement or achievement of their counseling treatment goals developed in collaboration with the ASW.

5.5.3 A minimum of ninety percent (90%) of CLIENTS who accept counseling services will begin Intake Assessment within thirty (30) days from referral dates.

5.5.4 CLIENTS who complete counseling services will increase knowledge of parenting and child development, and parental resilience, as identified in Subparagraphs 5.1.2 and 5.1.5 of this Attachment A.

6. REPORTING REQUIREMENTS

CONTRACTOR shall complete the following reporting requirements:

6.1 Assessment and Treatment Plan (ATP)

6.1.1 CONTRACTOR shall submit a type-written report, via SSA's Secure Communication Management System (SCMS), containing changes in CLIENT behavior necessary to achieve the goals identified during assessment, type and length of intervention planned, summary of contacts made during assessment, CLIENT's strengths, and community resource linkages. One (1) original report is required for each referral. Facsimiles shall not be accepted. A maximum of up to three (3), fifty-minute sessions per CLIENT may be used to complete the Intake Assessment. ATPs must be received by ADMINISTRATOR no later than sixty (60) calendar days from the referral stamp date.

6.1.2 Referrals automatically become inactive if the ATP is not received from CONTRACTOR within sixty (60) calendar days of the referral stamp date.

6.1.3 If a referral becomes inactive due to ADMINISTRATOR not receiving

the ATP within sixty (60) calendar days of the referral stamp date, CONTRACTOR will not be eligible to receive compensation for the referral, regardless of any services provided at any time.

6.2 Revised ATP

6.2.1 CONTRACTOR shall submit a Revised ATP type-written report to ADMINISTRATOR, within thirty (30) days, when a CLIENT's treatment goals or treatment plan require modification after the original ATP has been submitted. ASW must concur with the revised goals or plan prior to implementing the modification. A Revised ATP shall not extend the five (5) month service period.

6.3 Social and Family History

6.3.1 CONTRACTOR shall conduct a written assessment during the Intake process documenting the social and family history relevant to issues being addressed in counseling which includes, but is not limited to, obstacles to treatment, strengths, and motivation of individuals and family. The social and family history will include a mental status exam, substance abuse, and domestic violence evaluations. The written assessment will be maintained in CONTRACTOR's case notes.

6.4 Monthly Telephonic Progress Report

6.4.1 CONTRACTOR shall make monthly telephonic contact a minimum of one (1) time per month, directly with ASW for each referral regarding CLIENT's progress. Telephonic reports may include, but are not limited to: collateral contacts, changes in CLIENT behaviors, goals identified during assessment, description of specific examples of significant intervention efforts which have occurred, if any; and CLIENT's strengths, insights, community resource linkages, attendance, and other relevant CLIENT information. CONTRACTOR shall leave progress report, as described above, via voicemail, if unable to report directly to ASW. CONTRACTOR shall document monthly progress report including contact or attempted contact with ASW. The written report shall be

maintained in CONTRACTOR's case notes.

6.5 Termination Report (TR)

6.5.1 CONTRACTOR shall submit to ADMINISTRATOR, via SSA's Secure Communication Management System (SCMS), within thirty (30) days, a type-written comprehensive summary of all activity within the service period including: contacts made with CLIENT, ASW and collateral sources; all NS(s); CLIENT's status in meeting goals and objectives outlined in the ATP with specific descriptive examples of how progress was achieved, or not; all community resource linkages; CLIENT's behavioral changes, strengths, insights, attendance, and prognosis; identified issues for ASW regarding CLIENT's follow-up needs; and the reason services were terminated. One (1) TR is required for every referral.

6.6 Termination Report Without Intake for Unresponsive Client

6.6.1 A CLIENT is deemed unresponsive if within a thirty (30) day period CONTRACTOR does not receive any response after CONTRACTOR has placed at least three (3) telephone calls to, and mailed at least one (1) letter to CLIENT, and contacted ASW at least once, to request assistance in reaching CLIENT. CONTRACTOR shall document all attempted contacts to CLIENT and ASW in CONTRACTOR's case notes. At the end of the thirty (30) day period without CLIENT response, CONTRACTOR shall prepare and submit to RDM a TR Without Intake form. This completed form must reach RDM within sixty (60) days of the pre-authorized referral stamp date.

6.6.2 CONTRACTOR shall consult with ASW, and document consultation efforts made, prior to termination of a referral for any reason.

6.6.3 CONTRACTOR shall terminate a CLIENT upon written notice by ADMINISTRATOR.

7. CLIENT RECORDS

7.1 CONTRACTOR shall prepare and maintain accurate and complete records and documentation in case files of CLIENTS served, and dates and type of services

provided under this Contract in a form acceptable to SSA. All records shall be maintained in English, and English translation of all correspondence and forms shall be maintained in the case file for audits, and Utilization Reviews. CONTRACTOR shall file records in chronological order by open and closed cases, and labeled with case names and case numbers. CONTRACTOR shall prepare a separate case file for each referral received. Records and documentation prepared by CONTRACTOR shall be type-written and shall include, but not be limited to:

7.1.1 CLIENT's name, address, phone number, and employment information;

7.1.2 Names, birthdates, and gender of all family members;

7.1.3 Names of other persons in the home and their relationship to CLIENT;

7.1.4 COUNTY referral form and any referral documentation provided by ADMINISTRATOR;

7.1.5 Assessment and Treatment Plan;

7.1.6 Termination Report;

7.1.7 Extension Request and extension authorization, if applicable;

7.1.8 Case notes on a form provided by SSA;

7.1.9 Psychosocial History and Assessment;

7.1.10 Mental Status Examination;

7.1.11 Substance Abuse and Domestic Violence evaluation information;

7.1.12 Emergency contact information;

7.1.13 Special Incident Reports;

7.1.14 Community Resource Linkages;

7.1.15 Copies of all NS letters;

7.1.16 Financial Assessment and Sliding Fee Schedule;

7.1.17 Copies of third party insurance carriers and Medi-Cal disallowance/denial and reimbursement documentation;

7.1.18 Copies of Receipt for Service forms; and

7.1.19 Copies of Invoices/Claim forms.

8. FACILITY REQUIREMENTS

8.1 CONTRACTOR's office must be located in Orange County, California.

8.2 CONTRACTOR's office must provide a private room for services to ensure

CLIENT confidentiality is maintained.

8.3 CONTRACTOR's office location must be geographically proximate, preferably within a half-mile (880 yards) to a bus stop and near other forms of affordable public transportation.

8.4 CONTRACTOR's office shall be a family-friendly, safe, and age appropriate environment for children, youth, parents and caregivers.

8.5 CONTRACTOR shall be required to render counseling services in the office location provided or agreed to by ADMINSTRATOR. With SSA approval, CONTRACTOR may conduct pre-authorized services at a different location than CONTRACTOR's office.

9. UTILIZATION REVIEW

9.1 CONTRACTOR and ADMINISTRATOR's designee shall meet at least annually 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. CLIENT cases to be reviewed shall be randomly selected by ADMINISTRATOR and may include both open and closed cases.

9.2 ADMINISTRATOR may conduct a Utilization Review (UR) at CONTRACTOR's facility referenced in Paragraph 8.5**Error! Reference source not found.** 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.

9.3 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 Director of CFS for final resolution. Nothing in this subparagraph shall affect COUNTY's

termination rights under Paragraph 40 of this Contract.

10. TRAINING

10.1 COUNTY will not provide any reimbursement and will not be responsible for any expenses incurred by CONTRACTOR to participate in the orientation or any training.

10.2 CONTRACTOR shall be required to attend an orientation conducted by SSA prior to receipt of any referrals by ADMINISTRATOR.

10.3 ADMINISTRATOR may require CONTRACTOR to attend subsequent training if ADMINISTRATOR determines additional training is needed to provide services to CLIENTS, which may be presented or sponsored by COUNTY, or other training entities.

10.4 Licensed Marriage Family Therapist, Licensed Clinical Social Worker, and Licensed Professional Clinical Counselor CONTRACTORs shall remain in compliance with continuing education as determined by the BBS, maintain a valid and current license, and remain in good standing throughout the term of this Contract.

10.5 Clinical Psychologist CONTRACTORs shall remain in compliance with continuing education as determined by the BOP, maintain a valid and current license, and remain in good standing throughout the term of this Contract.

10.6 COUNTY will not be responsible for any training, continuing education, or licensure expenses incurred by CONTRACTOR throughout the term of this Contract.

11. COMPENSATION

11.1 COUNTY does not guarantee CONTRACTOR any specified minimum number of referrals or minimum sum of money during the term of this Contract. CONTRACTOR agrees to provide services requested, as determined by COUNTY, at fees listed in this Contract, regardless of the quantity of referrals received.

11.2 COUNTY shall pay CONTRACTOR, monthly in arrears, a rate of one hundred and twenty dollars ($120) per hour, for up to twenty (20) sessions of service, for the

following services:

11.2.1 Intake Assessment;

11.2.2 Individual counseling;

11.2.3 Conjoint and/or Family counseling, regardless of the number of CLIENTS served;

11.2.4 Pre-Authorized Extensions: After the first twenty (20) completed sessions, when pre-authorized extensions are on file with ADMINISTRATOR, COUNTY will reimburse CONTRACTOR for up to ten (10) additional sessions of service;

11.2.5 Actual time spent in Juvenile Court, on an active SSA case, and travel time to and from CONTRACTOR's office location;

11.2.6 Actual time spent in a CFT or TMO, and, if at a location other than CONTRACTOR's office location, travel time to and from CONTRACTOR's office location;

11.2.7 Referrals become eligible for compensation after an Intake Assessment session has been completed and SSA has received an original ATP;

11.2.8 Counseling sessions lasting less than fifty (50) minutes will be prorated in ten (10) minute increments;

11.2.9 Specialized Services (i.e., attendance at a CFT Meeting or TMO), shall be prorated in fifteen (15) minute increments; and

11.2.10 Compensation will be paid as stated in Subparagraph 11.2 above, less any applicable revenue, as specified in Paragraph 22 of this Contract.

11.3 CONTRACTOR shall be paid fifteen dollars ($15) per court letter, with written pre-authorization from ADMINISTRATOR.

11.4 No compensation will be made for the following:

11.4.1 Closed CFS cases.

11.4.2 Inactive referrals, regardless of any services provided at any time, including those referrals for which ATPs are submitted beyond sixty (60) calendar days from the pre-authorized referral stamp date.

11.4.3 Consultation time with County staff prior to receipt of the SSA pre-authorized referral form.

11.4.4 Counseling services provided to CLIENTS prior to pre-authorization date or after pre-authorization end date.

11.4.5 Counseling services provided for an authorized CLIENT requiring a crisis session if CONTRACTOR does not provide written justification to SSA within one (1) business day.

11.4.6 Services provided during the period of service suspension after a third NS and before written pre-authorized reinstatement is on file with SSA.

11.4.7 Actual time spent in Court pursuant to subpoena, on a closed case, nor travel time to and from CONTRACTOR's facility.

11.4.8 Client NS(s).

11.4.9 Mileage, parking, or any other travel costs related to case activities not included in compensable costs.

11.4.10 CONTRATOR's time, mileage, parking, or any other costs related to attending orientation/training session.

11.4.11 Neuropsychological, psychological, or any other types of diagnostic testing and/or diagnostic evaluations.

11.4.12 Preparation, participation, or any other activities related to URs.

11.4.13 Postage, supplies, or any other costs related to maintaining case activities.

12. CLAIMS

12.1 Claims shall include original signatures. Claims shall not be accepted by facsimile.

12.2 All claims shall be accompanied by a properly completed Receipt for Services form for each referral claimed, signed and dated on the day services are provided by both CONTRACTOR and all adult CLIENTS receiving services. The parent/caregiver or other responsible adult present must sign and date on behalf of minors receiving services.

12.3 All claims for payment shall include all supporting documents, including but not limited to, one (1) RFS form for each referral claimed, two (2) copies of each ATP, two (2) copies of each TR, and one (1) copy of each NS Letter.

12.4 Claims typically include all services provided during the previous calendar month. When the initial three Intake (3) sessions of a new referral occur over a two (2)

month period (i.e., two (2) sessions in May and one (1) session in June), the claim will include RFS forms from a two (2) month period for the new referral only.

12.5 Claims for time spent in Juvenile Court must be accompanied by a copy of the subpoena requiring CONTRACTOR to appear in Juvenile Court. If the court date on the subpoena does not match the date and time spent in court, a written explanation, from CONTRACTOR, must be attached.

12.6 Claims for Crisis Sessions are documented on the RFS and claimed on the standard invoice form.

12.7 Claims for Specialized Services including CFT Meetings, TMO's, Court Letters, and/or travel time, must be submitted on a Specialized Service Detail form provided by RDM.

12.8 It is at the sole discretion of ADMINISTRATOR whether any compensation will be paid due to special circumstances.

13. SERVICES DELIVERY DISPUTE RESOLUTION

13.1 In the event CONTRACTOR and ADMINISTRATOR are unable to resolve differences of opinion regarding the necessity and/or appropriateness of services, length of treatment, and/or timeliness of required treatment reports the parties may attempt to resolve the dispute in the following order:

13.1.1 CONTRACTOR and ASW shall first attempt to resolve the dispute.

13.1.2 If CONTRACTOR and ASW are unable to resolve the dispute, CONTRACTOR and CFS Senior Social Services Supervisor shall attempt to resolve the dispute.

13.1.3 COUNTY's Program Manager (PM) or designee shall have the final right and sole discretion to resolve any dispute as to the necessity and appropriateness of services, the length of treatment, and/or timeliness of required treatment reports. The decision of COUNTY's PM or designee shall be final.

13.1.4 In the event a complaint is received regarding CONTRACTOR, CONTRACTOR shall comply with an investigation and/or UR and final decision by ADMINISTRATOR.

13.1.5 ADMINISTRATOR shall have sole discretion in placing CONTRACTOR on a do-not-refer status and reassigning current CLIENTS to another CONTRACTOR pending outcome of an investigation and/or UR.

13.2 Nothing in this subparagraph shall affect COUNTY's termination rights under Paragraph 40 of this Contract.

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. County of Orange Information Technology Security Guidelines: County of Orange security standards follows 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 the requirements of the County of Orange Information Technology Security Guidelines ("Security Guidelines") attached hereto as Exhibit 1 and incorporated herein by reference, as existing or modified, that pertain to Contractor in connection with the Services performed by Contractor as set forth in the scope of work of this Contract. Any violations of such Security Guidelines shall, in addition to all other available rights and remedies available to County, be cause for immediate termination of this Contract. Such Security Guidelines include, but are not limited to this Attachment.

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 Guidelines:** 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
1055 N. Main St., 6th Floor
Santa Ana, CA 92701
Phone: (714) 567-7611
Andrew.Alipanah@ocit.ocgov.com

Linda Le, CHPC, CHC, CHP
County Privacy Officer
1055 N. Main St., 6th Floor
Santa Ana, CA 92701
Phone: (714) 834-4082
Linda.Le@ocit.ocgov.com

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

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.

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.

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.

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

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.

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.

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

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:

- 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@$SWoRd13

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.

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.

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.

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.

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

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.

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

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.

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.

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.

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.

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.

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.

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.

6.2.14 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.