

Contract MA-063-26010267
For
Short-Term Residential Therapeutic Program at Tustin Family
Campus
Between
Social Services Agency
And
Rite of Passage Adolescent Treatment Centers and Schools, Inc.



MA-063-26010267
BETWEEN
COUNTY OF ORANGE
AND
RITE OF PASSAGE ADOLESCENT TREATMENT CENTERS AND SCHOOLS, INC.
FOR THE PROVISION OF
SHORT-TERM RESIDENTIAL THERAPEUTIC PROGRAM AT TUSTIN FAMILY
CAMPUS

This Contract is by and between the COUNTY OF ORANGE, hereinafter referred to as “County,” and RITE OF PASSAGE ADOLESCENT TREATMENT CENTERS AND SCHOOLS, INC., a Nevada non-profit corporation, qualified to transact interstate business in the State of California, hereinafter referred to as “Contractor.”

ATTACHMENTS

This Contract is comprised of this document and the following Attachments, which are attached hereto and incorporated by reference into this Contract:

Attachment A – Scope of Work

Attachment B – Information Technology Security Provisions

Attachment C - Information Technology Security Guidelines

Attachment D – SSA State Privacy and Security Provisions

RECITALS

WHEREAS, County issued a Request for Proposal for Short-Term Residential Therapeutic Program services at Tustin Family Campus in October of 2025;

WHEREAS, County desires to contract with Contractor for the provision of Short-Term Residential Therapeutic Program services at Tustin Family Campus;

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

WHEREAS, such services are authorized and provided for pursuant to Section 16501 of the Welfare and Institutions Code; and

ACCORDINGLY, THE PARTIES AGREED AS FOLLOWS:

ARTICLES

TERMS AND CONDITIONS - SOCIAL SERVICES AGENCY-HUMAN SERVICES

1. TERM

The term of this Contract shall commence on July 1, 2026, and terminate on June 30, 2029, unless earlier terminated pursuant to the provisions of the Terminations paragraph of this Contract; however, Contractor shall be obligated to perform such duties as would normally extend beyond this term, including, but not limited to, obligations with respect to indemnification, audits, reporting and accounting. This Contract may be renewed thereafter for a two-year term upon mutual agreement of both parties. The County does not have to provide a reason if it elects not to renew this Contract.

2. ALTERATION OF TERMS

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

- A. 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.
- B. 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.
- C. Contractor certifies it is in compliance with Disabled Veteran Business Enterprise requirements at the time this Contract is executed.

4. DESCRIPTION OF SERVICES

- A. Contractor agrees to provide those services, facilities, equipment, and supplies, as described in Attachment A to the Contract between County of Orange and Rite of Passage Adolescent Treatment Centers and Schools, Inc., for the Provision of Short-Term Residential Therapeutic Program Services at Tustin Family Campus, attached hereto and incorporated herein by reference. Contractor shall operate continuously throughout the

term of this Contract with the number and type of staff described and as required for provision of services hereunder.

- B. Subject to 30 days advance written notice, County may require changes in staffing allocations to reflect current workload demands or service needs as long as County's maximum funding obligation, as set forth in this Contract, is not exceeded.
- C. Upon the request of County, Contractor shall send appropriate staff to attend an orientation session and subsequent training sessions given by County.

5. **COMPLIANCE WITH LICENSING STANDARDS AND LAWS**

- A. Contractor warrants that it has 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 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 County within one business day of any change in license or permit status (e.g., becoming expired, inactive, etc.).
- B. Contractor represents and warrants that services to be provided under this Contract shall fully comply, at Contractor's expense, with all standards, laws, statutes, restrictions, ordinances, requirements, and regulations (collectively "laws"), including, but not limited to, those issued by County in its governmental capacity and all other laws applicable to the services at the time services are provided to and accepted by County. Contractor acknowledges that County is relying on Contractor to ensure such compliance, and pursuant to the requirements of the Insurance and Indemnification section, Contractor agrees that it shall defend, indemnify and hold County and County Indemnitees harmless from all liability, damages, costs and expenses arising from or related to a violation of such laws. Contractor shall remain in compliance and in good standing, maintaining current and active business entity and/or nonprofit registration status, with all applicable federal, state and local registration requirements at the time of execution of the contract through the duration of the term of the Contract, and shall provide annual confirmation of current and active status to County through the term of the Contract.
- C. 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; Title 48 CFR Section 31.2; 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.
- D. Contractor shall be licensed as a Short-Term Residential Therapeutic Program (STRTP) and Contractor shall operate in compliance with the California Department of Social Services (CDSS)/Community Care Licensing Division (CCLD) STRTP licensing

standards and all administrative regulations, rules, and policies adopted thereunder, as each and all may now exist or be hereafter amended.

1. Contractor shall notify County 60 days prior to any request Contractor makes to CDSS to change their license, including, but not limited to, changes in site location, population served, and capacity.
 2. Contractor shall notify County within 72 hours if CDSS or SSA substantiates findings on investigation involving Contractor or Contractor's staff, and/or if action is being taken against the Contractor's license by CDSS.
- E. For federally funded Contracts in the amount of \$25,000 or more, Contractor certifies that its officers and/or principals are not debarred or suspended from federal financial assistance programs and/or activities.
- F. Contractor shall cooperate with CDSS on the implementation, monitoring, and evaluation of the State's Child Abuse and Neglect Prevention and Intervention Program, and shall comply, to the mutual satisfaction of County and CDSS, with any and all reporting and evaluation requirements established by CDSS.

6. DELEGATION AND ASSIGNMENT/CHANGE OF OWNERSHIP

A. Delegation and Assignment

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 10 percent 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.
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.

B. Change of Ownership

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

7. SUBCONTRACTS

No performance of this Contract or any portion thereof may be subcontracted or otherwise delegated by Contractor, in whole or in part, without first obtaining the prior express written consent of County. Any attempt by Contractor to subcontract or delegate any performance of this Contract without the prior express written consent of County shall be invalid and shall constitute a material breach of this Contract, and any attempted assignment or delegation in derogation of

this paragraph shall be void. In the event that Contractor is authorized by County to subcontract, this Contract shall take precedence over the terms of the agreement between Contractor and subcontractor, and any agreement between Contractor and a subcontractor shall incorporate by reference the terms of this Contract. Contractor shall remain responsible for the performance of this Contract and indemnification of County notwithstanding the County’s consent to Contractor’s request for approval of a subcontractor. Under no circumstances shall County be required to directly monitor the performance of any subcontractor. All work performed by a subcontractor must be monitored by Contractor and must meet the approval of the County of Orange pursuant to the terms of this Contract.

8. FORM OF BUSINESS ORGANIZATION/NAME CHANGE

A. Form of Business Organization

1. Upon the request of County, Contractor shall prepare and submit, within 30 days thereafter, an affidavit executed by persons satisfactory to County, containing, but not limited to, the following information:
 - a. The form of Contractor’s business organization, i.e., proprietorship, partnership, corporation, etc.
 - b. A detailed statement indicating the relationship of Contractor, by way of ownership or otherwise, to any parent organization or individual.
 - c. 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.

B. Change in Form of Business Organization

1. 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 County, 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.

C. Name Change

1. 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. USE OF COUNTY PROPERTY

- A. County intends to permit Contractor the use of office space, office furniture, and office equipment located at the Tustin Family Campus at which Contractor shall be co-located

with County staff pursuant to this Contract, as is more particularly set forth in that certain lease or license agreement described in Subparagraph 9.B, below. As stated in the lease or license agreement, said office space, office furniture, and equipment shall be used solely by employees of Contractor while performing their assigned duties pursuant to this Contract.

- B. Contractor shall enter into a lease or license agreement with County for facilities provided by County and shall execute all terms and conditions of said agreement upon County's presentation of said document to Contractor. Failure to execute the lease or license agreement will result in a breach of this Contract.
- C. Contractor is responsible for any costs associated with Fair Employment and Housing Act and Americans with Disabilities Act accommodations for its own employees at County facilities. County may, at its sole discretion and on a case-by-case basis, provide for such accommodations at no cost to Contractor.

10. NON-DISCRIMINATION

- A. 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.
- B. Contractor shall furnish any and all information requested by County and shall permit County access, during business hours, to books, records, and accounts in order to ascertain Contractor's compliance with this Non-Discrimination section of this Contract.
- C. Non-Discrimination in Employment
 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).
 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.
 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)

D. Non-Discrimination in Service Delivery

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 this Non-Discrimination section of this Contract.
2. Contractor shall provide any and all clients desirous of filing a formal complaint any and all information as appropriate:
 - a. Pamphlet: “Your Rights Under California Welfare Programs” (PUB 13)
 - b. Discrimination Complaint Form
 - c. Civil Rights Contacts
 - County Civil Rights Contact:
 Orange County Social Services Agency
 Program Integrity
 Attn: Civil Rights Coordinator
 P.O. Box 22001
 Santa Ana, CA 92702-2001
 Telephone: (714) 438-8877
 - State Civil Rights Contact:
 California Department of Social Services

Civil Rights Bureau
P.O. Box 944243, M/S 8-16-70
Sacramento, CA 94244-2430
Telephone: (916) 654-2107
Toll Free: (866) 741-6241

Federal Civil Rights Contact:

Office for Civil Rights
U.S. Department of Health and Human Services
90 7th Street, Suite 4-100
San Francisco, CA 94103
Customer Response Center: (800) 368-1019

- d. The following websites provide Civil Rights information, publications and/or forms:
 - i. <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)
 - ii. <http://www.cdss.ca.gov/inforesources/Civil-Rights/Your-Rights-Under-California-Welfare-Program> (Pub 13 – Your Rights Under California Welfare Programs)
 - iii. <http://ssa.ocgov.com/about/services/contact/complaints/comply> [Social Services Agency (SSA) Contractor and Vendor Compliance page]

11. NOTICES

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:

Rite of Passage Adolescent Treatment Centers and Schools, Inc.
2560 Business Parkway, Suite B
Minden, NV 89423

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

- A. Deposited in the United States mail, first class postage prepaid and addressed as shown above;
- B. Sent by Email;

- C. Faxed and transmission confirmed; or
- D. Accepted by U.S. Postal Services Express Mail, Federal Express, United Parcel Service, or any other expedited delivery service.

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.

12. 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 business day, give notice thereof, including all relevant information with respect thereto, to the other party.

13. INDEMNIFICATION

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 its/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.

14. INSURANCE

- A. 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 and provide Certificates of Insurance and endorsements to County during the entire term of this Contract.
- B. Contractor shall ensure that all subcontractors performing work on behalf of Contractor pursuant to this Contract shall be covered under Contractor's insurance as an Additional Insured or maintain insurance subject to the same terms and conditions as set forth herein for Contractor. Contractor shall not allow subcontractors to work if subcontractors have less than the level of coverage required by County from Contractor under this Contract. It is the obligation of Contractor to provide notice of the insurance requirements to every subcontractor and to receive proof of insurance prior to allowing any subcontractor to begin work. Such proof of insurance must be maintained by Contractor through the entirety of this Contract for inspection by County representative(s) at any reasonable time.
- C. 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.

D. If Contractor fails to maintain insurance acceptable to County for the full term of this Contract, County may terminate this Contract.

E. Qualified Insurer

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).
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.
3. The policy or policies of insurance maintained by Contractor shall provide the minimum limits and coverage as set forth below.
4. Increased insurance limits may be satisfied with Excess/Umbrella policies. Excess/Umbrella policies when required must provide Follow Form coverage.

F. Required Coverage Forms

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

G. Required Endorsements

1. Commercial General Liability policy shall contain the following endorsements, which shall accompany the Certificate of Insurance:
 - a. 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.
 - b. 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.
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.

3. The Network Security and Privacy Liability policy shall contain the following endorsements which shall accompany the Certificate of Insurance.
 - a. An Additional Insured endorsement naming the County of Orange, its elected and appointed officials, officers, employees, and agents as Additional Insureds for its vicarious liability.
 - b. A primary and non-contributory endorsement evidencing that the Contractor's insurance is primary, and any insurance or self-insurance maintained by the County shall be excess and non-contributing.
- H. 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.
- I. Contractor shall provide 30 days prior written notice to the County of any policy cancellation or non-renewal and 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.
- J. If Contractor's Network Security & Privacy Liability and/or Professional Liability policy are a "claims made" policy, Contractor shall agree:
 1. The retroactive date must be shown and must be before the date of the Contract or the beginning of the Contract services.
 2. Insurance must be maintained, and evidence of insurance must be provided for at least three years after expiration or earlier termination of Contract services.
 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 years after expiration of earlier termination of the Contract.
- K. 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).
- L. Insurance certificates should be forwarded to County at the address indicated in Notices section of this Contract.
- M. If Contractor fails to provide the insurance certificates and endorsements within seven days of notification by CEO/County Procurement Office or Deputy Procurement Agent, award may be made to the next qualified proponent.
- N. 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.
- O. 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 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.

- P. 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.

<u>COVERAGE</u>	<u>MINIMUM LIMITS</u>
Commercial General Liability	\$1,000,000 per occurrence \$2,000,000 aggregate
Automobile Liability including coverage for owned or scheduled, non-owned, and hired vehicles: Passenger Vehicles up to four (4) passengers, not including the driver Passenger Vehicles up to seven (7) passengers, not including the driver Passenger Vehicles for eight (8) or more passengers, not including the driver	 \$1,000,000 per occurrence \$2,000,000 per occurrence \$5,000,000 per occurrence
Workers' Compensation	Statutory
Employer's Liability Insurance	\$1,000,000 per accident or disease
Network Security and Privacy Liability	\$1,000,000 per claims-made
Professional Liability Insurance	\$1,000,000 per claims-made or occurrence \$1,000,000 aggregate
Sexual Misconduct Liability	\$1,000,000 per occurrence

15. NOTICE OF LITIGATION, INCIDENTS, CLAIMS, OR SUITS

Contractor shall report to County, in writing within 24 hours of occurrence, the following:

- A. 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.

- B. 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.
- C. Any third-party claim or lawsuit filed against Contractor arising from or relating to services performed by Contractor under this Contract.
- D. Any injury to an employee of Contractor that occurs on County property.
- E. 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.
- F. 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.

16. CONFLICT OF INTEREST

- A. Contractor shall exercise reasonable care and diligence to prevent any actions or conditions that could result in a conflict with the best interests of County. This obligation shall apply to Contractor, Contractor's officers, directors, employees, agents, and subcontractors associated with accomplishing work and services hereunder. Contractor's efforts shall include, but not be limited to establishing precautions to prevent 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 from acting in the best interests of County.
- B. Contractor shall notify County, in writing, of any potential or actual conflicts of interest between Contractor and County that may arise prior to, or during the period of, Contract performance, including, but not limited to, whether any known County public officer's child is an officer or director of, or has an ownership interest of 10 percent or more in, Contractor. 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 upon request by County.
- C. County of Orange Board of Supervisors policy prohibits its employees from engaging in activities involving a conflict of interest. Contractor shall not, during the period of this Contract, employ any County employee for any purpose.

17. 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.

18. SUPPLANTING GOVERNMENT FUNDS

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

19. EQUIPMENT

- A. Computer Equipment - No computers and/or personal electronic devices, such as tablets and laptop computers, or any component thereof, may be purchased with funds provided under this Contract.

20. BREACH SANCTIONS

- A. 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, County may, and in addition to immediate termination and any other remedies available at law, in equity, or otherwise specified in this Contract:
 1. Afford Contractor a time period within which to cure the breach, which period shall be established by County; and/or
 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
 3. Offset against any monies billed by Contractor but yet unpaid by County those monies disallowed pursuant to Subparagraph 1.2 above.
- B. County will give Contractor written notice of any action pursuant to this Paragraph, which notice shall be deemed served on the date of mailing.

21. PAYMENTS

- A. Allowable Costs

During the term of this Contract, County shall pay Contractor monthly in arrears, the rate of reimbursement for the services provided under this Contract, as established by the State of California, as stated in CDSS Manual of Policies and Procedures, Division 11, Chapter 11-425.1. Payments will accrue from the date a Foster Youth/NMD is placed, and terminate on the date before the Foster Youth/NMD is discharged, removed, runs away, or otherwise leaves the TFC. No payment will accrue to Contractor if the Foster Youth/NMD is placed in and removed from the TFC and placed in another facility on the same day, i.e., the Foster Youth/NMD must spend the night in the TFC before payment will accrue.

- B. It is mutually understood that an approved STRTP Contractor shall be reimbursed at the STRTP rate, as determined by CDSS in accordance with WIC Section 11462(c) or any new rate structure implemented by CDSS through legislation.
- C. Upon prior written approval of the Foster Youth's/NMD's County Social Worker, County may continue to pay for residential care for up to 14 days when a Foster Youth/NMD leaves the TFC prior to the planned discharge date (e.g., runaway), if Contractor has agreed to

take the Foster Youth/NMD back immediately upon notice during the period of continued payment.

- D. Contractor shall provide written notice to the Orange County Foster Care Eligibility Team immediately, and no later than within 30 days of the receipt of a payment for an Orange County placement, which is inconsistent with the period of placement and results in an overpayment or an underpayment. The overpayment or underpayment will be identified by the Foster Youth's/NMD's name, case number, caseload number, and the amount of underpayment or overpayment.

22. OVERPAYMENTS

- A. Contractor shall provide written notice to the Children and Family Services Foster Care Eligibility unit within 30 days of receipt of a payment for an Orange County placement that is inconsistent with the actual period of placement and results in an overpayment or underpayment. The overpayment or underpayment shall be identified by the Foster Youth's/NMD's name, case number, caseload number, and the amount of underpayment and/or overpayment.

- B. Any payment(s) made by the County to Contractor in excess of that to which Contractor is entitled under this Contract shall be repaid to the 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 the County which result from a payment by any other funding source shall be repaid, at the discretion of Administrator, to the County or the funding source. Unless earlier repaid, Contractor shall make repayment within 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 the County by the funding source, then Contractor shall reimburse the County within 30 days thereafter and prior to any administrative appeal process. Contractor agrees to pay all costs incurred by the County necessary to enforce the provisions set forth in this Paragraph.

- 1. Contractor may call the following phone numbers with overpayment/underpayment questions:

Social Services Agency: Foster Care Program Development
(714) 704-8866 or (714) 704-8441

- 2. Contractor may call the following phone numbers to appeal overpayment/underpayment matters:

Social Services Agency: Program Integrity
(714) 438-8880 or
California Department of Social Services:
State Hearing System
(800) 952-5253

23. OUTSTANDING DEBT

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

24. MEDICAL COSTS

- A. Contractor shall enroll in subscription coverage programs, as applicable, that provide emergency care response services, including paramedic assessment services, in the city or county, where facility is located.
- B. Contractor shall seek reimbursement for Foster Youth/NMD medical costs from the State Medi-Cal program during such periods as the Foster Youth/NMD is eligible for health care services under that program.
 1. If the Foster Youth/NMD is ineligible for Medi-Cal services, Contractor shall notify Foster Youth/NMD's County Social Worker and specify the medical treatment needed and approximate cost.
 2. Except in emergencies, authorization by the County Social Worker shall be obtained prior to incurring any medical expenses not covered by Medi-Cal.
 3. County may pay for medical services, in accordance with County procedure, if such services are deemed necessary by County and Medi-Cal rejects coverage. County will reimburse Contractor for medical expenses paid by Contractor pursuant to this section based on Medi-Cal rates.
 4. Contractor shall be responsible for controlling the use of each Foster Youth/NMD's Medi-Cal proof-of-eligibility card.

25. EARLY AND PERIODIC SCREENING DIAGNOSIS AND TREATMENT PROGRAM

County will maximize the use of Early and Periodic Screening Diagnosis and Treatment Program (EPSDT) funding when children and families are determined to have an eligible condition. County will provide training for Contractor on EPSDT charting requirements and will facilitate the processing of EPSDT funding claims. Contractor shall comply with these requirements for EPSDT eligible children and their families and shall facilitate the processing of EPSDT funding claims. Contractor understands that in order to participate in this funding opportunity, contracts with both County of Orange Social Services Agency and County of Orange Health Care Agency shall be required.

26. FINAL REPORT

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

27. INDEPENDENT AUDIT

- A. Contractor shall employ a licensed certified public accountant who shall prepare and file with County an annual organization-wide audit of related expenditures during the term of this Contract in compliance with 31 USC 7501 – 7507, as well as its implementing regulations under 2 CFR Part 200, Uniform Administrative Requirements, Cost Principles and Audit Requirements for Federal Awards. If Contractor is not subject to the aforementioned regulations for any year covered during the term of this Contract, Contractor shall provide County an Independent Auditor's Report of Contractor's financial statements. The audit must be performed in accordance with generally accepted government auditing standards. Contractor shall cooperate with County, State, and/or federal agencies to ensure that corrective action is taken within six months after issuance of all audit reports with regard to audit exceptions.

28. RECORDS, INSPECTIONS AND AUDITS**A. Financial Records**

1. Contractor shall prepare and maintain accurate and complete financial records. Financial records shall be retained by Contractor for a minimum of five years from the date of final payment under this Contract, or until all pending County, State, and federal audits are completed, whichever is later.
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 County.

B. Client Records

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 County.
2. Contractor shall keep all County data provided to Contractor during the term(s) of this Contract for a minimum of five 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 the Termination provisions of this Contract.
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.

C. Public Records

1. 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.

D. Inspections and Audits

1. The U.S. Department of Health and Human Services, Comptroller General of the United States, Director of CDSS, State Auditor-General, County, 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.
2. Contractor shall make its books and records available within the borders of Orange County within 10 days of receipt of written demand by County.
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.
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.

- E. 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.

29. PERSONNEL DISCLOSURE

- A. This Paragraph applies to all of Contractor's personnel providing services through this Contract, paid and unpaid, including those identified in the Staffing section of this Contract (hereinafter referred to as “Personnel”).
- B. Contractor shall make available to County a current list of all Personnel providing services hereunder, including résumés and job applications. Changes to the list will be immediately provided to County, in writing, along with a copy of a résumé and/or job application. The list shall include:
 1. Names and dates of birth of all Personnel by title, whose direct services are required to provide the programs described herein;
 2. A brief description of the functions of each position and the hours each person works each week, or for part-time Personnel, each day or month, as appropriate;
 3. The professional degree, if applicable, and experience required for each position; and

4. The language skill, if applicable, for all Personnel.
- C. Where authorized by law, and in a manner consistent with California Government Code Section 12952, Contractor shall require prospective Personnel to provide detailed information regarding the conviction of a crime, by any court, for offenses other than minor traffic offenses. Information discovered subsequent to the hiring or promotion of any prospective Personnel shall be cause for termination from the performance of services under this Contract.
- D. 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).
- E. Where authorized by law, Contractor shall conduct, at no cost to County, a criminal record background check on all Personnel who will have direct, interactive contact with clients served through this Contract. Background checks conducted through the California Department of Justice shall include a check of the California Central Child Abuse Index, when applicable. Candidates will satisfy background checks consistent with this Paragraph and their performance of services under this Contract.
- F. Contractor shall ensure that clearances and background checks described above in Subparagraphs 29.D and 29.E are completed prior to Contractor's Personnel providing services under this Contract.
- G. In the event a record is revealed through the processes described in above Subparagraphs 29.D and 29.E, County will be available to consult with Contractor on appropriateness of Personnel providing services through this Contract.
- H. Contractor warrants that all Personnel assigned by Contractor to provide services under this Contract have satisfactory past work records and/or reference checks indicating their ability to perform the required duties and accept the kind of responsibility anticipated under this Contract. Contractor shall maintain records of background investigations and reference checks undertaken and coordinated by Contractor for Personnel assigned to provide services under this Contract, for a minimum of five years from the date of final payment under this Contract, or until all pending County, State, and federal audits are completed, whichever is later, in compliance with all applicable laws.
- I. Contractor shall immediately notify County 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. County may determine whether such Personnel may continue to provide services under this Contract and shall provide notice of such determination to Contractor in writing. Contractor's failure to comply with County's decision shall be deemed a material breach of this Contract, pursuant to the Breach Sanctions section of this Contract.
- J. County has the right to approve or disapprove all of Contractor's Personnel performing work hereunder, and any proposed changes in Contractor's Personnel.

- K. County shall have the right to require Contractor to remove any Personnel from the performance of services under this Contract. At the request of County, Contractor shall immediately replace said Personnel.
- L. Contractor shall notify County immediately when Personnel is terminated for cause from working on this Contract.
- M. Disqualification, if any, of Contractor Personnel, pursuant to this Paragraph shall not relieve Contractor of its obligation to complete all work in accordance with the terms and conditions of this Contract.

30. 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.

31. CHILD AND DEPENDENT ADULT/ELDER ABUSE REPORTING

Contractor shall establish a procedure acceptable to County 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.

32. 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.

33. CONFIDENTIALITY

- A. Contractor agrees to maintain the confidentiality of its records pursuant to WIC Sections 827, 362.5 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.
- B. All records and information concerning any and all persons referred to Contractor by County or County's designee shall be considered and kept confidential by Contractor and Contractor's employees, agents, subcontractors, and all other individuals performing services under this Contract. Contractor shall require all of its employees, agents, subcontractors, and all other individuals performing services under this Contract to sign an agreement with Contractor before commencing the provision of any such services, agreeing to maintain confidentiality pursuant to State and federal law and the terms of this Contract.
- C. 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.
- D. Contractor agrees that any and all subcontracts entered into shall be subject to the confidentiality requirements of this Contract.
- E. 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.
 - 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.
 - 2. Contractor must receive prior written approval of the Juvenile Court before allowing any Foster Youth/NMD 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.

34. SECURITY

Contractor shall abide by the requirements in Attachment B - Information Technology Security Provisions, Attachment C - Information Technology Security Guidelines, and Attachment D – SSA State Privacy and Security Provisions.

35. 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.

36. WAIVER

No delay or omission by either party hereto to exercise any right or power accruing upon any noncompliance or default by the other party with respect to any of the terms of this Contract shall impair any such right or power or be construed to be a waiver thereof. A waiver by either of the parties hereto of any of the covenants, conditions, or agreements to be performed by the other shall not be construed to be a waiver of any succeeding breach thereof, or of any other covenant, condition, or agreement herein contained.

37. SERVICES DURING EMERGENCY AND/OR DISASTER

- A. 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.
- B. 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.
- C. 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.
- D. 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.

38. PUBLICITY, LITERATURE, ADVERTISEMENTS AND SOCIAL MEDIA

- A. 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.
- B. Contractor may develop and publish information related to this Contract where all of the following conditions are satisfied:

1. County provides its written approval of the content and publication of the information at least 30 days prior to Contractor publishing the information, unless a different timeframe for approval is agreed upon by the County;
2. Unless directed otherwise by County, the information includes a statement that the program, wholly or in part, is funded through County, State, and Federal Government funds;
3. The information does not give the appearance that the County, its officers, employees, or agencies endorse:
 - a. Any commercial product or service; and
 - b. Any product or service provided by Contractor, unless approved in writing by Administrator; and
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 County. 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://ocit.oc.gov/egovernment-policies>.

39. REPORTS

- A. Contractor shall provide information deemed necessary by County to complete any State-required reports related to the services provided under this Contract.
- B. 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 County, upon a form approved by County. The County may modify the provisions of this Paragraph upon written notice to Contractor.

40. 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).

41. 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:

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

- B. 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
- C. It will notify County and EPA about any known violation of the above laws and regulations.

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

Contractor shall be in compliance with Section 319 of Public Law 101-121 pursuant to 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 County that includes the text below.

- A. The undersigned certifies to the best of his or her knowledge and belief that:
 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.
 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.
 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.
 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

43. 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.

44. TERMINATION PROVISIONS

- A. County may terminate this Contract without penalty, immediately with cause or after 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 County of the right to terminate this Contract shall relieve County of all further obligations under this Contract.
- B. For 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 County 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.
- C. 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.
- D. 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, County may immediately terminate this Contract, reduce County's maximum funding obligation, or modify this Contract, without penalty. The decision of County shall be binding on Contractor. County will provide Contractor with written notification of such determination. Contractor shall immediately comply with County's decision.
- E. 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.

45. 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.



46. SIGNATURE IN COUNTERPARTS

- A. 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.
- B. 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.

SIGNATURE PAGE

IN WITNESS WHEREOF, the Parties hereto have executed this Contract the date set forth opposite their signatures.

Contractor: RITE OF PASSAGE ADOLESCENT TREATMENT CENTERS AND SCHOOLS, INC.

<small>DocuSigned by:</small>			
	Lawrence Howell	Executive Director	3/5/2026 9:43:35 AM PST
<small>4B7E7A365A2D41D...</small>	Name	Title	Date
<small>Signed by:</small>			
	CJ BOWER	Chief Financial officer	3/5/2026 11:20:43 AM PST
<small>428F929C8622426...</small>	Name	Title	Date

COUNTY OF ORANGE, a political subdivision of the State of California

COUNTY AUTHORIZED SIGNATURE:

<small>Deputy Procurement Agent</small>			
Signature	Name	Title	Date

Approved as to form:
County Counsel

<small>DocuSigned by:</small>			
	Carolyn Frost	Deputy	3/6/2026 9:27:49 AM PST
<small>D3AB98D76D0B425...</small>	Name	Title	Date

ATTACHMENT A - SCOPE OF WORK

1. POPULATION TO BE SERVED

Contractor shall provide Short-Term Residential Therapeutic Program (STRTP) services at the Tustin Family Campus (TFC) to Foster Youth/Non-Minor Dependents (NMD) referred by County pursuant to the terms and conditions set forth herein, and in accordance with Contractor's Plan of Operation/Program Statement approved by the California Department of Social Services (CDSS), Community Care Licensing Division (CCLD) and incorporated herein by reference as it currently exists or may hereafter be amended. The population to be served as defined in this Paragraph shall hereinafter be referred to as "Foster Youth/NMD" and may include:

- A. Orange County Juvenile Court dependent Foster Youth, 12 to 18 years old, pursuant to Welfare and Institutions Code (WIC) Section 241.1, or have dual status jurisdiction pursuant to WIC 241.1, with specific age range to be in accordance with Contractor's facility approved CDSS/CCLD STRTP license.
- B. Orange County Juvenile Court NMDs, who are under the age of 18 years old upon placement, and are 18 years old to 21 years old, with an open SSA case, pursuant to WIC Section 11400(v)(1)(2)(3), or have dual status jurisdiction.
- C. NMDs that meet "medical necessity" as defined in Subparagraph 2.Y of this Scope of Work, for STRTP level of intervention as determined through the Interagency Placement Committee process.
 - 1. A Foster Youth who turns 18 years old while placed in the STRTP TFC and meets NMD criteria, may remain placed in the STRTP TFC only if attending high school. After high school graduation or when the NMD reaches the age of 19 years old, whichever comes first; the NMD placement must be terminated unless the NMD meets "medical necessity" as verified by County.
- D. At-risk Foster Youth/NMDs who may have a history of child abuse, loss, and/or trauma; multiple placement failures; significant behavioral issues, with or without associated "medical conditions" as defined in Subparagraph 2.X of this Scope of Work; significant mental health needs; dual diagnosis; psychiatric hospitalizations; and medication non-compliance.
- E. Foster Youth/NMDs who are classified as Commercially Sexually Exploited Children (CSEC) as defined in Subparagraph 2.H of this Scope of Work.
- F. Foster Youth/NMDs who would otherwise be placed in another STRTP facility licensed by CDSS/CCLD.

2. DEFINITIONS

- A. Authorized Absence: An absence of which the Foster Youth/NMD's County Social Worker has authorized and/or has mutual agreement for absence with Contractor.
- B. Authorized Representative: A Foster Youth/NMD's County Social Worker, Probation Ward's assigned County Probation Officer, and/or other parties designated by the Orange County Juvenile Court to represent a Foster Youth/NMD's interest on their behalf.

- C. Case Plan: A written document which identifies a case plan goal, objectives to be achieved, services to be provided, case management activities to be performed, and placement needs and transition.
- D. Child and Family Team (CFT): As defined in WIC Section 16501, a group of individuals who are convened by the placing agency and who are engaged through a variety of team-based processes to identify the strengths and needs of the child or youth and their family, and to help achieve positive outcomes for safety, permanency, and well-being.
- E. Child and Adolescent Needs and Strengths (CANS) Tool: A multi-purpose tool development for children's services to support decision making, including level of care and service planning, to facilitate quality improvement initiatives, and to allow for the monitoring of outcomes and services.
- F. Children and Family Services (CFS): A division of the County of Orange Social Services Agency (SSA).
- G. Clinical Staff: Individuals who possess a valid license as a Psychologist, Clinical Psychologist, Licensed Clinical Social Worker, Licensed Marriage and Family Therapist, Psychiatrist, or any other licensed professional whose California license permits the design and/or implementation of behavior modification intervention services, including specialty mental health services, and mental health supports, as appropriate to the needs of the Foster Youth/NMD.
- H. Commercially Sexually Exploited Children (CSEC): A commercially sexually exploited or sexually trafficked child, as described in California Penal Code (CPC) Section 236.1, is one who receives food or shelter in exchange for, or is paid to, perform sexual acts described in CPC Sections 236.1 or 11165.1, and whose parent or guardian failed to or was unable to protect the child. At-risk foster youth are those whose living circumstances may subject them to becoming victims of commercial sexual exploitation.
- I. Community Care Licensing Division (CCLD): The division of the CDSS that is responsible for the licensing and monitoring of STRTPs for compliance with CCL regulations and standards within the State of California.
- J. County Social Worker: SSA employee assigned as the case-carrying social worker responsible for a Foster Youth/NMD's placement and care.
- K. Culturally Responsive: The 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 different 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.
- L. Dual Status Jurisdiction: Foster Youth/NMD designated by the Orange County Superior Court or Juvenile Court, as one who falls under Court jurisdiction under both WIC Section 300 and Sections 601, 602, or is receiving services under Probation supervision and therefore may be supervised by and receive services from both SSA and the Probation Department, based on Orange County Juvenile Court Protocol for WIC Section 241.1

proceedings. SSA is the lead placement agency for dual status jurisdiction Foster Youth/NMDs served by the STRTPs on the Tustin Family Campus.

- M. Emergency Placement: A Foster Youth/NMD placed into a STRTP on an emergency basis prior to a determination by the Interagency Placement Committee (IPC) and/or Qualified Individual (QI) that the Foster Youth/NMD qualifies for STRTP level of services.
- N. Family Finding and Engagement (FFE): Permanency strategies designed to promote, establish, and strengthen a foster youth's connections with family members and other supportive adults who can provide relational permanency.
- O. Foster Youth: An individual between the ages of birth to 18 years old, referred for foster care services.
- P. Health and Education Passport (HEP): The document that provides historical and current medical, dental and behavioral health, and educational information as it pertains to a Foster Youth/NMD.
- Q. HEP Encounter Forms: The form to record the Foster Youth's/NMD's medical/dental exam information for the Health Passport Update report.
- R. Important Persons: Individuals identified by the Foster Youth/NMD placed in STRTPs, as defined in WIC Section 366.3(e)(2), that are important to the Foster Youth/NMD consistent with his/her best interest.
- S. Individual Education Plan: The plan for a student's specialized educational program, including performance assessment, identified goals, and specific services.
- T. Interagency Placement Committee (IPC): A multidisciplinary team composed of the County Placing Agency (Probation or CFS), Health Care Agency, and other agencies. The IPC certifies that the Foster Youth/NMC has been assessed as meeting medical necessity criteria for Medi-Cal Specialty Mental Health Services, or has been assessed as seriously emotionally disturbed, or has been identified as having behavioral or treatment needs that can only be met by the level of care provided in a STRTP.
- U. Interim Licensing Standards for STRTP (ILS): A set of written instructions and standards issued by the CDSS that governs the provisions of Short-Term Residential Therapeutic Programs.
- V. Lead Agency: SSA is the lead agency who assumes responsibilities for placement of the Foster Youth/NMD at the STRTP TFC in cases where Dual Status Jurisdiction is invoked as the disposition.
- W. Lower Level of Care: The least restrictive environment from a residential facility, including, but not limited to, any of the following: reunification with biological parent(s); placement with relatives, or non-related extended family members (NREFMs); placement in a resource family home; transitional housing program; supervised independent living program; or emancipation.
- X. Medical Conditions: Those medical conditions that are not considered acute or chronic health problems for Foster Youth/NMDs that do not meet criteria requiring therapeutic intervention and skilled nursing care during all or part of the day, and do not meet criteria

to be considered "medically fragile" or have "special health care needs" as defined in Health and Safety Code Section 1760.2(b), and WIC Section 17731.

- Y. Medical Necessity: A physical or mental state as determined by County, that limits an NMD's ability to participate in any one of the following activities: completing high school or an equivalency program; enrollment in post-secondary education or vocational school; participation in a program or activity that promotes or removes barriers to employment; and/or employment of at least 80 hours per month.
- Z. Medi-Cal: California's Medicaid public health insurance program which provides medical services, mental health, and substance use disorder services, including behavioral health treatment, for children and adults with limited income.
- AA. National Accreditation: An accreditation pursuant to Title 22, Division 6, Interim Licensing Standards (ILS), Section 87089. STRTP must obtain accreditation for their STRTP from an entity identified by CDSS.
- BB. Needs and Services Plan (NSP): A time limited, goal oriented written plan, which identifies the specific needs of an individual Foster Youth/NMD, required by Title 22, Division 6, Interim Licensing Standards (ILS), Sections 87068.2 and 87068.22, and delineates those services necessary in order to meet the Foster Youth/NMD's identified needs.
- CC. Non-Minor Dependent (NMD): A Foster Youth who is at least 18 years old and not more than 21 years old, or a non-minor former dependent or ward, as defined in WIC Section 11400(v). The NMD must meet at least one of the participation requirements in WIC Section 11403(b) and must participate in a Transitional Independent Living Plan (TILP) under the supervision of County.
- DD. Placing Agency: The lead agency, SSA, is responsible for placement of all Foster Youth/NMD, including those with Dual Status Jurisdiction, and is responsible for case management and Court-related matters, and as defined in Health and Safety Code Section 1536.1.
- EE. Plan of Operation and Program Statement: The document prepared by a STRTP as required by State regulation and filed with CDSS/CCLD, which provides details of the day-to-day operation of the STRTP, including, but not limited to, staffing, training, therapy, intake criteria, and record-keeping.
- FF. Probation Department: The Orange County Probation Department.
- GG. Probation Officer: The Foster Youth/NMD's assigned Probation Department Case Manager.
- HH. Program Manager: SSA management staff responsible for the oversight of STRTP placements.
- II. Short-Term Residential Therapeutic Program (STRTP): A residential facility operated by a public agency or private organization and licensed by the CCLD, pursuant to WIC Section 1562.01 and Chapter 7.5 of the ILS, that provides an integrated program of specialized and intensive care and supervision, services, support and treatment, twenty-four (24) hours a day, seven (7) days per week.

JJ. Special Education Local Planning Area (SELPA): A service area covered by a special education local plan and the governance structure created under any of the planning options of California Education Code Sections 56205, 56206, 56208, 56213, 56241, and 56243-56245. SELPAs facilitate educational programs and services for special needs students and training for parents and educators.

KK. Strengthening Families Protective Factors: “Strengthening Families” is a research-informed approach developed by the Center for the Study of Social Policy to increase family strengths, enhance child development and reduce the likelihood of child abuse and neglect. It is based on engaging families, programs, and communities in building five protective factors: parental/caregiver resilience, social connections, knowledge of parenting and child development, concrete support in times of need, and social and emotional competence of children. This approach assists child welfare systems, early education, prevention organizations, and other programs work with parents to build five protective factors that, when present, increase the overall well-being of children and families.

LL. Title 22: Title 22, California Code of Regulations (CCR), Division 6, Chapter 1, General Licensing Requirements, relating to the licensing of community care facilities and STRTPs.

MM. Transitional Independent Living Plan (TILP): A plan established by the County Social Worker in collaboration with the Foster Youth/NMD to develop and document meaningful and attainable goals that will support the Foster Youth/NMD’s transition to adulthood and meet at least one participation requirement for the NMD to remain eligible for Extended Foster Care.

NN. Transitional Planning Services Program (TPSP): A program within the CFS Division of SSA which provides independent living skills training resources, supportive services, vocational assessment referrals, and financial resources assistance for employment and education to Orange County’s dependent, NMD and emancipated Foster Youth, ages 16 through 20 years old.

OO. Tustin Family Campus (TFC): A multi-treatment residential facility designed to serve as a community based collaborative resource for children, youth, young adults, and their families, to provide strength-based, family-friendly, and family-centered services.

PP. Unauthorized Absence: An event, absence without leave (AWOL), where a Foster Youth/NMD's whereabouts are unknown by Contractor's staff or has run away from placement.

QQ. Visitors: Volunteers, repairmen, family members, friends, consulting staff, outside agency staff, or any other person who is not a resident or staff member of the STRTP TFC.

3. GOALS, STRATEGIES, AND OUTCOME OBJECTIVES

A. Goals

1. Foster Youth/NMDs will achieve and demonstrate mental health stabilization with the intent of successfully transitioning to a Lower Level of Care in order to achieve:

- reunification with biological parent(s); placement with relatives, NREFMs, or RFA homes; placement to transitional housing; or emancipation.
- a. Mental health stabilization shall be measured through Foster Youth/NMD's goals as outlined in their NSP, which are measurable and time tracked. NSP goals are reviewed and shared at each CFT meeting with the Foster Youth/NMD's treatment team who provide input and recommendations for transition planning and stepping down to a Lower Level of Care.
2. Per STRTP guidelines, Contractor shall facilitate and assist Foster Youth/NMDs in achieving and demonstrating sustainable and increased level of social, emotional, and behavioral functioning within six months, to support the intent of successfully transitioning from the STRTP TFC and be maintained in a Lower Level of Care.
 - a. If the CFT determines that the Foster Youth/NMD will not be ready to transition to a Lower Level of Care upon the sixth month of placement, or the Foster Youth/NMD's 180th day in residential treatment, the County Social Worker will request an extension with Child Welfare Director approval.
 3. Contractor shall provide STRTP core services and support services needed to stabilize the Foster Youth/NMD's behavior to reduce time in residential treatment; allow the Foster Youth/NMD to live and learn successfully in the STRTP, classroom, and community; achieve a successful placement; and provide the Foster Youth/NMD with skills to become a self-sufficient adult.

B. Strategies

1. Contractor shall incorporate the following Five Protective Factors Framework from the Strengthening Families research-informed approach, developed by the Center for the Study of Social Policy, in providing services and evaluating outcomes to increase family strengths, enhance child development, and reduce the likelihood of child abuse and neglect:
 - a. Parental/Caregiver Resilience
 - b. Social Connections
 - c. Knowledge of Parenting and Child Development
 - d. Concrete Support in Times of Need
 - e. Social and Emotional Competence of Children
2. Because mental health treatment and substance abuse treatment services have been identified as a Protective Factor that support the social and emotional competence of children, Contractor shall:
 - a. Participate as requested by County in research and/or evaluation studies designed to show the effectiveness of their treatment program.
 - b. Collaborate with County to establish and provide outcome measures as they become necessary to meet program goals and objectives. Outcome measures may include, but are not limited to: surveys, tracking logs, pre-tests and post-tests, and evaluation tools.

- c. County measurement tools are subject to change based on program and evaluation needs, as defined by County.

C. Outcome Objectives

1. Contractor shall be expected to meet the following outcomes during the term of the resulting contract:
 - a. A minimum of 80 percent of Foster Youth/NMDs shall attend monthly CFT meetings until the Foster Youth/NMDs transition into permanent or long-term care settings or as directed by County.
 - b. A minimum of 90 percent of Foster Youth/NMDs shall have a customized Individual Needs and Services Plan developed within 30 days of intake into the STRTP.
 - c. As a result of Contractor's FFE efforts, a minimum of 70 percent of Foster Youth/NMDs who reside in this care setting for longer than one month shall establish and/or maintain a connection with a family member, natural support person, or individual who is important to the Foster Youth/NMD who is committed to being a lifelong support for the Foster Youth/NMD, or will establish a connection with a mentor or other community member who is committed to being a monthly support person for the foster child.

4. HOURS OF OPERATION

- A. Contractor shall provide STRTP services 24 hours a day, seven days a week.

5. GENERAL REQUIREMENTS

A. Plan of Operation/Program Statement

1. Contractor shall prepare and maintain a current, written plan of operation pursuant to ILS Section 87022 that meets all standards and includes a Program Statement pursuant to ILS Section 87022.1.
2. Contractor shall submit to County a copy of any new or revised Program Statement.

B. STRTP Accreditation

1. Contractor shall obtain national accreditation pursuant to ILS Section 87089 and provide a copy of the Accreditation Certificate to County.
2. Contractor shall notify County of any change of status in its national accreditation within 10 business days of receiving notification from the accrediting entity.

C. Referrals

1. It is mutually understood that no minimum number of placement referrals is guaranteed, expressed, or implied, under this Contract. Contractor agrees to provide services as requested by County, regardless of the quantity of placement referrals received.

2. Contractor shall only accept referrals from County for placements at the STRTP TFC homes.
3. SSA shall be the lead agency for Foster Youth/NMDs with dual status jurisdiction.
4. Contractor shall not discriminate against Foster Youth/NMDs based on their sexual orientation/gender identity. Contractor shall collaborate with County on which STRTP TFC home best serves the Foster Youth/NMD's needs.
5. Contractor shall provide all programmatic services to disabled Foster Youth/NMDs, including, but not limited to, specialized and individualized services in consultation with County.
6. Contractor and County shall negotiate the referrals considering County's placement needs and Contractor's CDSS/CCLD approved Plan of Operation/Program Statement.
7. Upon Contractor receiving a placement referral from County, Contractor shall evaluate and notify County within 48 hours regarding the decision for placement. Contractor shall:
 - a. Review referral, intake packet, and reports;
 - b. Review and discuss Foster Youth/NMDs identified strengths; maladaptive behaviors, triggers, and coping skills; supports; and mental health needs; and
 - c. Interview the Foster Youth/NMD as a part of the screening process, when possible and appropriate.
8. Once Contractor accepts placement, Contractor shall provide STRTP services until Foster Youth/NMD is removed or the Foster Youth/NMD transitions to an alternate placement, including to a Lower Level of Care.
9. Accepted Referrals
 - a. Once referral is accepted for placement, the referral shall be forwarded to Contractor's intake process.
 - b. Contractor shall follow admission requirements pursuant to CDSS/CCLD STRTP ILS and California Department of Health Care Services (CDHCS) regulations.
10. Declined Referrals
 - a. If Contractor declines a placement referral, Contractor shall submit to County within five business days, written documentation in a format acceptable to County, the reasons for declining referral and details on identified resources/services/supports or change of circumstance which may enable acceptance of placement.
 - b. After an initial placement referral is declined, County may request a reconsideration for the declined referral through a second level review.
 - c. If after a second level review placement cannot be facilitated, Contractor shall submit to County within three business days, written documentation in a format acceptable to SSA, the clinical justification for declined referral.
11. Emergency Placement Referrals

- a. Contractor shall accept Emergency Placement referrals and provide services to individuals referred by County for designated Emergency Placements pursuant to WIC Sections 11462.01(h)(3)(A) and 4096(g)(2)(A).
- b. Following Emergency Placement of the Foster Youth/NMD in the facility, if it is determined the facility cannot continue to provide necessary services or meet the needs of the Foster Youth/NMD, then Contractor shall continue to provide residential care to the Foster Youth/NMD for the amount of time necessary to identify and transition the Foster Youth/NMD to an alternative, suitable placement.

D. Contractor Performance Monitoring

- 1. Contractor’s performance shall be monitored and reviewed by County who will conduct ongoing reviews as part of an ongoing evaluation of Contractor’s performance.
- 2. Contractor shall cooperate with County in providing the information necessary for performance monitoring.
- 3. County may use a variety of inspection methods to evaluate Contractor’s performance, including, but not limited to, the following:
 - a. County will inspect Contractor cases and applicable data reports to ensure compliance with the goals, strategies, and outcome objectives, as stated in Paragraph 3 of this Scope of Work;
 - b. Random sampling of program activities, including a review of case files;
 - c. Review of activity checklists;
 - d. Conduct random in-person observations;
 - e. Inspection of output items on a periodic basis, as deemed necessary; and
 - f. Review of Foster Youth/NMD complaints, SIRs, and/or Foster Youth/NMD questionnaires.
- 4. When it is determined that the services were not performed in accordance with the resulting Contract and/or County policies during the review period, County may require a corrective action plan. Contractor shall, within the time period specified in any such corrective action plan, remedy the performance defects.
- 5. Contractor shall cooperate with County in providing the information necessary for performance monitoring and with authorized state and/or federal representatives who may audit program services.
- 6. Performance evaluation meetings shall be conducted, as deemed necessary by County.

6. SERVICE REQUIREMENTS

Contractor shall provide the following services:

A. Specialty Mental Health Services

- 1. Provide specialty mental health services to Foster Youth/NMDs in accordance with Contractor’s approved Plan of Operation and Program Statement.

2. Provide a mental health program approved by the CDHCS or from a delegated county Mental Health Plan.
3. Provide specialty mental health and additional treatment services for Foster Youth/NMDs who meet medical necessity criteria for specialty mental health services under Medi-Cal eligibility, as described in Title 9, CCR Chapter 11, Section 1830.210.
4. Ensure that psychiatric needs of a Foster Youth/NMD are met in accordance with the Medi-Cal program and CCLD regulations to the extent that funding and services are available.
5. Ensure provision of mental health services to Foster Youth/NMDs, including, but not limited to:
 - a. Individual, collateral, and/or group therapy;
 - b. Family therapy, when applicable;
 - c. Mental health services to address CSEC, when applicable;
 - d. Assessment for substance use treatment services;
 - e. Crisis intervention;
 - f. Case management;
 - g. Psychiatric evaluation; and
 - h. Psychotropic medication management.
6. Provide assistance in locating and referring Foster Youth/NMDs to Day Rehabilitation, Day Treatment Intensive, Crisis Stabilization, and Therapeutic Behavioral Services, when recommended by the CFT and/or required by the NSP or treatment plan.
7. Provide individual and/or group counseling to Foster Youth/NMD, consistent with the NSP or as directed by the CFT.
 - a. Contractor shall provide counseling case management services onsite at the residential facility and provide mental health crisis management support by clinical staff 24 hours a day, seven days a week, on-call, in-person, and by telephone.
 - b. If the Foster Youth/NMD declines to attend counseling, Contractor shall attempt to engage Foster Youth's/NMD's participation in counseling, and document engagement attempts in the Foster Youth/NMD's case record, pursuant to ILS 87070(b).

B. Transition Services

1. Contractor shall provide transition support services to Foster Youth/NMDs and families upon initial entry, placement changes, and to families who assume permanency through reunification, adoption, or guardianship, in accordance with ILS Sections 87078.1(a)(2), 87068.2(a) and (c), and 87068.22.
2. Contractor shall ensure that Foster Youth/NMD and his/her/their Authorized Representative have the opportunity to participate in the development of a transition plan informed by the CFT.

C. Family Foster Youth/NMDs Important Person Relationships

1. Collaborate with County to encourage Foster Youth’s/NMD’s relationship with family members and/or other individuals who are important to a Foster Youth/NMD, with the knowledge and concurrence of the assigned Social Worker/Probation Officer as indicated in the Foster Youth's/NMD’s permanency plan.
2. Assist County personnel and/or County’s Family Finding and Engagement (FFE) contracted staff to help identify, research, and connect Foster Youth to parties identified as Important Persons by the CFT and cleared through County. This includes, but is not limited to, social media searches, facilitation of phone contact, monitoring visitation, or other means as outlined and approved by County.
3. Keep record of family and NREFM contacts, or any other significant relationship connections or Important Persons relevant to reunification and permanency and alert County to new or potential Important Persons.

D. Education, Physical, Behavioral, Mental Health, and Extracurricular Supports

Contractor shall provide educational, physical, behavioral, and mental health supports, including extracurricular activities and social supports, in accordance with Title 22 CCR, ILS Sections 87067, 87068.2, 87068.22, 87072, 87078, 87078.1 and 87079.

1. Education Supports

Contractor shall:

- a. Enroll Foster Youth/NMD in the local school, school of origin, or private program (the latter only if funding is provided by County or other third-party payer) within three school days of placement. Contractor shall notify County within three business days of any obstacles preventing the Foster Youth/NMD’s enrollment in school.
- b. Cooperate with the SELPA for any needed assessment and follow-up for special education services through the development and implementation of an IEP and surrogate parent appointment, as appropriate.
- c. Monitor Foster Youth/NMD’s attendance and performance in school and credits earned and assess progress to determine areas in which improvement is needed. Contractor shall document monthly the Foster Youth/NMD’s academic and social performance, and document date of contact, contact person, and feedback provided as well as steps taken to address any deficiency or areas of concern.

2. Physical, Behavioral, Mental Health, and Extracurricular Supports

Contractor shall:

- a. Adhere to County policies provided by CFS, including, but not limited to, obtaining Orange County Juvenile Court consent for psychotropic medications in a form approved by County, and that all Orange County Juvenile Court requirements for psychotropic medication administration, documentation, monitoring, and reporting responsibilities are followed.
- b. Document the Foster Youth/NMD's participation in extracurricular activities that include, but not limited to, organized sports, cultural events, and artistic programs.

Contractor shall maintain receipts for extracurricular activities and provide to County upon request.

- c. Take Foster Youth's/NMD's HEP Encounter Form and HEP to all medical and dental appointments and ensure that medical history is shared with the health care provider to update records.
 - i. Contractor shall provide the health care provider with the HEP Encounter Form(s) to complete.
 - ii. Contractor shall submit the completed HEP Encounter Form(s) to the County.

3. Behavioral and Mental Health Crisis

Contractor shall:

- a. Coordinate, develop, and implement protocol for emergency behavioral and mental health crises, including, but not limited to, evaluation, mental health intervention, crisis management and support during regular business, and after-hours; 24 hours a day, seven days a week, for direct services staff and clinical staff.
- b. Utilize a certified behavioral crisis prevention, crisis management, and crisis intervention program approved by CDSS/CCLD and County.

4. Transitional Planning Services Program (TPSP)

Contractor shall:

- a. Work collaboratively with SSA's TPSP/Independent Living Program (ILP) and SSA's contracted Emancipation/ILP service provider(s) to meet the service goals set forth in each Foster Youth/NMD's TILP.
- b. Provide transportation for Foster Youth/NMDs to and from all TPSP related activities as required by County, and provide supervision for three or more Foster Youth/NMDs attending the same activity.
- c. Document participation in all activities, contacts with TPSP, other independent living programs, and any programs offered by Contractor, for each Foster Youth/NMD, and provide information to County upon request.

5. Permanency Support Services

Contractor shall:

- a. Provide services to facilitate achieving permanency for Foster Youth/NMD, including supporting efforts for reunification, achieve adoption or guardianship, and efforts to establish and/or maintain relationships with Foster Youth/NMD'S social support network which may include, but not limited to: biological parent(s), siblings, extended relatives, NREFMs, peers, tribes, other significant relationship connections, or other Important Persons to the Foster Youth/NMD as appropriate; and identified in the NSP in collaboration with the CFT, and in accordance with Title 22 CCR, ILS.
- b. Continue family finding efforts and engagement practices to assist Foster Youth/NMD in identifying, developing, and maintaining important relationships, provided that such relationships are in the Foster Youth/NMD's best interests and are consistent with Foster Youth/NMD's Case Plan.

6. Indian Child Services

- a. Contractor shall ensure that Indian Foster Youth/NMDs receive core services and support, in accordance with the Federal Indian Child Welfare Act. These services shall be in the best interests of Indian Foster Youth/NMDs, including Culturally Responsive, child-centered practices that respect Native American history, culture, retention of tribal membership, and connection to the tribal community and traditions.

7. Additional Services and Supports

Contractor shall:

- a. Provide STRTP Nursing staff oversight as described in Paragraph 12 of this Scope of Work, to Foster Youth/NMDs including those with “medical conditions” referred by County.
- b. Work collaboratively with County to deliver trauma informed, strength-based, linguistically and culturally responsive, developmentally appropriate, permanency focused, family-friendly, and family-centered STRTP services that address the individually assessed needs of Foster Youth/NMDs.
- c. Coordinate and facilitate monthly CFT meetings which may include CFT members, including, but not limited to: Foster Youth/NMD, immediate and extended family members, and persons of significance to the Foster Youth/NMD, representatives from SSA, Probation Department, Health Care Agency, school district representatives, and other service providers.
- d. Submit a written summary to County of each CFT meeting, in a format acceptable to County, no later than seven calendar days after each meeting is held.
- e. Ensure that appropriate behavioral and mental health, services, as specified in Section 1830.210 of Title 9, of the CCR, and resources are provided by initiating an individualized NSP with a focus on placement stability and step-down services, including, but not limited to:
 - i. Personal accountability and self-control;
 - ii. Problem-solving techniques;
 - iii. Developing adaptive, self-regulating coping skills;
 - iv. Replacing high-risk behaviors with alternative, healthy behaviors;
 - v. Fostering self and community awareness;
 - vi. Developing positive interpersonal and social skills;
 - vii. Decreasing/mitigating runaway behaviors and other high-risk behaviors;
 - viii. Self-sufficiency skills;
 - ix. Educational preparedness; and
 - x. Independent living.
- f. Provide monitored and supervised visitation when ordered by Orange County Juvenile Court.

- g. Assist and mentor Foster Youth/NMD on how to obtain essential documents such as California Driver's License and/or Identification Card, Social Security Card, or medical card.

E. Clothing

1. Provide an ongoing monthly clothing allowance of no less than \$75.00 per Foster Youth/NMD, to be used to purchase new clothing necessary to meet the Foster Youth's/NMD's basic needs in a manner appropriate to his/her age, social environment, and daily activities.
2. Ensure the Foster Youth/NMD has a minimum of a five day supply of clothing upon Intake. If a Foster Youth/NMD enters the facility with less than a five day supply, Contractor shall supply the minimum clothing requirements.
3. Provide the ongoing monthly clothing allowance 30 days after placement and every month thereafter.
4. Allow clothing allowance to be used for purchase of a Foster Youth/NMD's replacement clothes and/or mandatory uniforms.
5. Provide reserved/unused clothing allowance to Foster Youth/NMD upon Foster Youth/NMD's discharge in a form to be determined by County. Contractor shall apply a pro-rated daily rate of \$2.50 to determine the clothing allowance due to the Foster Youth/NMD, should the Foster Youth/NMD leave Contractor's care prior to the completion of the monthly clothing allowance cycle.
6. Document all clothing purchases and retain receipts in Foster Youth's/NMD's case file.
7. Ensure Foster Youth/NMD has adequate clothing upon Foster Youth/NMD's request to reserve unused monthly clothing allowance. If Contractor approves Foster Youth/NMD's request to reserve funds, Contractor shall document the amount of rollover funds which shall include documentation of Foster Youth/NMD's acknowledgment and signature.
8. Conduct and document inventory of Foster Youth/NMD's clothing and personal property upon initial placement and when Foster Youth/NMD transitions/discharges out of placement. Inventory documentation shall be maintained in the Foster Youth/NMD's case file.
9. Conduct and document clothing inventory each quarter to assess Foster Youth/NMD's needs. Updates to the inventory shall be made when new clothing items are purchased and when items are discarded. Foster Youth/NMD and Contractor staff shall sign the updated inventory.
10. Follow minimum clothing requirements as determined by County.

F. Personal Property

1. Unless directed otherwise by County, all Foster Youth/NMDs shall take their clothing, cash resources, reserved clothing allowance, personal property, and valuables with them when placement is terminated.

2. If the Foster Youth/NMD is unable to take the above items upon placement termination, clothing and personal property shall immediately be stored separately and securely for each individual Foster Youth/NMD by Contractor for a maximum period of 30 calendar days, after which it shall be delivered to the Foster Youth/NMD's County Social Worker.
3. At termination of placement, Contractor shall provide an appropriate method of transport for clothing and personal property, such as luggage or canvas-type duffel bags (not trash or paper/plastic bags).
4. Provide a copy of the final inventory at termination to County and/or receiving party.
5. Provide a list of items removed from Foster Youth/NMD's possession due to safety concerns or that were considered to be contraband to the Foster Youth/NMD's Social Worker/Probation Officer and mutually agree to disposition of item. Items may include, but are not limited to, large cash resources, drug paraphernalia, electronic items, etc.

G. Food and Emergency Supplies

1. Foster Youth/NMD shall receive an adequate and balanced diet as required by the ILS Section 87076 guidelines.
2. Contractor shall maintain emergency First Aid/Earthquake supplies, as outlined in Title 22 CCR, Section 80075, and as deemed appropriate by County.
3. Contractor shall maintain the following emergency supplies, at minimum, per Foster Youth/NMD on the premises:
 - a. One week supply of staple nonperishable foods;
 - b. Two day supply of fresh perishable foods; and a minimum five day supply of at least one gallon of water per day.

H. Chores

1. Contractor shall specify and post reasonable chores which Foster Youth/NMD will be required to do as part of their regular routine. Any and all other chores are to be voluntary.
2. Foster Youth/NMD's County Social Worker may review Contractor's policies regarding chores, and disapprove, if appropriate, the chores assigned to a specific Foster Youth/NMD.
3. Foster Youth/NMD shall be supervised by Contractor while they are engaged in any assigned chores.

I. Minimum Allowances

1. Contractor shall provide each Foster Youth/NMD with a minimum allowance as set forth below no less frequently than once a week and such allowance shall be documented in each Foster Youth/NMD's case file. Receipt of such allowance shall be initialed by Foster Youth/NMD. Weekly minimum allowance may be increased at the discretion of the County with 30 days written notice to Contractor.

Age Weekly Allowance Rate

12 years	\$12.00
13 years	\$13.00
14 years	\$14.00
15 years	\$15.00
16 years	\$16.00
17 years	\$17.00
18 years	\$18.00
19+ years	\$19.00

J. Safeguards for Cash Resources, Personal Property, and Valuables

1. Contractor shall assist each Foster Youth/NMD in keeping cash resources, personal property, and valuables separate and intact in accordance with Title 22 CCR, Section 80026.
2. Contractor shall maintain accurate records of cash resources, personal property, and valuables.
3. In the event that Foster Youth/NMD is employed, Contractor shall assist Foster Youth/NMD in setting up a bank account in accordance with ILS Section 87072(c)(11), to the satisfaction of the Foster Youth's/NMD's Social Worker/Probation Officer. Foster Youth's/NMD's funds shall not be commingled with Contractor's funds or petty cash.
4. Contractor shall develop a system for monitoring Foster Youth/NMD's bank funds for accounts where Contractor's staff has authority to access account. Such system should include:
 - a. A monthly, two party verification process to safeguard funds of the Foster Youth's banking accounts from deposits or withdrawals not authorized by Foster Youth.
 - b. Verification of monitoring and authorized signatures.
 - c. Account records shall be retained in Contractor's case record maintained for the Foster Youth/NMD.

K. Transportation

1. Contractor shall provide transportation for Foster Youth/NMD as required or approved by County, including, but not limited to:
 - a. Court appearances upon receiving Notice of Hearing;
 - b. Visitation appointments;
 - c. School and/or school activities (including school of origin, as ordered by the Court and/or recommended by the CFT);
 - d. Medical, dental, therapeutic, or psychiatric appointments;
 - e. Extracurricular activities; and
 - f. Other activities as informed by Foster Youth's/NMD's CFT.

2. Contractor shall notify assigned Social Worker/Probation Officer or Authorized Representative if Foster Youth/NMD utilizes any form of transportation not provided by Contractor.
3. Contractor shall not utilize taxi cabs or other ridesharing services such as Uber or Lyft, unless approved by assigned Social Worker/Probation Officer.

L. Drug Testing

1. Contractor shall collaborate with the Foster Youth's/NMD's County Social Worker and/or Probation Officer if drug testing of a Foster Youth/NMD is deemed by the Juvenile Court to be necessary.
2. Contractor shall not perform drug testing of Foster Youth/NMD placed in Contractor's facility by County without Juvenile Court authorization or parental consent.

M. Notice of Request for Change of Placement

1. Contractor shall submit written notice to County at least 14 calendar days prior to placement change.
 - a. Written notice shall be on Contractor's letterhead and completed by the STRTP TFC Head of Service, or their clinical designee.
 - b. Written notice shall include steps and efforts taken to maintain placement and specialty mental health services offered and/or provided.
 - c. Written notice shall provide detailed explanation for the need to change placements, and reasons the STRTP TFC can no longer meet the therapeutic needs of the Foster Youth/NMD.
2. A CFT meeting shall be conducted prior to any placement change, planned or unplanned. Contractor shall attend and participate in any CFT meetings resulting from a Foster Youth's/NMD's placement change/removal.
3. CFT meetings regarding placement change shall be conducted by a facilitator and in a location determined by County.

N. Removal of Transfer of Foster Youth/NMD

1. County may remove, with or without stating cause, any or all Foster Youth/NMD placed with Contractor.

O. Law Enforcement Contact

1. If Contractor contacts law enforcement officials regarding any issue related to the provision of services under the resulting Contract, County shall immediately telephone Foster Youth's/NMD's Social Worker/Probation Officer, STRTP Program Manager, or designee, and parent(s)/guardian(s) to provide a verbal report.
2. Contractor shall follow the verbal report with the submission of a written Special Incident Report of the issue involving law enforcement, in a form approved by County, to Foster Youth's/NMD's Social Worker/Probation Officer and STRTP Program Manager, or designee, and CFS STRTP Liaison/Probation Monitor.

- a. Contractor shall submit the Special Incident Report within three calendar days of the incident via the Secured Foster Youth Information Database (FYI system), or FAX to (714) 935-7725 if FYI system is unavailable for Foster Youth/NMDs involved with Probation Department.
- b. County may request Contractor to send Special Incident Reports to additional designees, as deemed appropriate by County.

P. Other Contractor Responsibilities

1. Visitors

Contractor shall establish a set of rules regarding visitors in compliance with CDSS/CCLD, maintain a separate Visitors Log Book for each STRTP TFC home, and shall ensure the following:

- a. Maintain each STRTP TFC home Visitors Log Book pursuant to Subparagraph 8.B of this Scope of Work.
 - b. Document visitation hours, sign-in/sign-out, and designated visitation areas in the Visitors Log Book. Such rules shall apply to all visitors and visiting areas.
 - c. Upon entering each STRTP TFC home, all visitors shall be required to sign in on the Visitor's Log Book. Contractor staff shall request a valid California Driver's License or other form of government issued picture identification and shall record the name, address, and driver's license number, or identification number, if available, of each visitor as well as the visitor's relationship to the Foster Youth/NMD, the stated purpose of the visit, and the time of the visitor's entry and departure. Unaccompanied visiting minors shall be supervised by Contractor staff.
 - d. Parent(s)/guardian(s), relatives, or Important Persons of the STRTP TFC Foster Youth/NMD's, who have been approved by the County Social Worker for unmonitored visitation, shall be accompanied by Contractor's staff to and from a private designated location in the STRTP TFC home where the visit will take place. In these instances, Contractor's staff need not be present during the visit.
2. Contractor shall develop and maintain community involvement through collaborative partnerships with local Community Based Organizations, including, but not limited to, Faith Based Organizations, Family Resource Centers, middle schools, high schools, community colleges, four-year colleges and universities, potential employers, One-Stop Centers, Orangewood Foundation, independent living skills service providers, vocational training programs, and housing authorities.
 3. Contractor shall post Medi-Cal Certification notices as required by the State of California, and post safety notices and other literature as indicated by County. Such notices and literature may be in the form of, but not limited to, placards, posters, checklists, instructions, or diagrams.

Q. After Care

Contractor shall provide individualized discharge planning, as directed by the CFT, and Contractor shall include the following after care services:

1. Collaborative assessment/step-down/transition process from Contractor staff to other providers or specialists, to enhance communication of Foster Youth/NMD information, and facilitate continuity of treatment between providers and/or programs.
 - a. After care planning should include, but not be limited to, coordination with medical providers, mental health specialists, educational and vocational services, and housing resources that align the with Foster Youth's/NMD's individualized NSP to ensure a stable and supported transition.

7. **FACILITIES**

- A. Contractor may serve a maximum of 12 Foster Youth/NMDs at the two STRTP TFC homes located at 15405 Lansdowne Road, Tustin, California, 92782.
 1. Each STRTP TFC home shall serve a maximum of six Foster Youth/NMDs, regardless of gender.
 2. The living area for each home is approximately 3,827 square feet of living space, and the garage is approximately 770 square feet.
 - a. Each home contains three residential bedrooms; each bedroom is approximately 131 square feet and each bedroom is set up to accommodate two occupants.
 - b. Each home contains two full bathrooms and one half bathroom to be shared by all occupants.
 - c. Each home contains an activity/dining area, kitchen, pantry, and laundry area for all occupants, and an office for Contractor staff.
 - d. Each home is equipped with commercial grade appliance and residential furniture.
 - e. Each home includes an attached apartment with two bedrooms, a bathroom, living room, and a kitchen/dining area.
 3. Contractor shall be required to enter into a Real Estate License Agreement with the County (Lease, Sublease, License/Permit, or any other real estate agreement deemed necessary by County), based on fair market rental rates. Contractor shall be required to pay the monthly rent, which is currently estimated to be \$5,424.46 per month, per home (\$1.18 per square foot, modified gross), for a total of \$10,848.92 per month.
 4. Based upon mutual benefit to Contractor and to County, there will be no monthly rent from the date the resulting contract commences through the first full calendar month following the date, or, when the first Foster Youth/NMD is placed. Contractor shall notify County's Facilities Services Manager immediately in writing when the first Foster Youth/NMD is placed and will commence payment of rent as provided therein. The anticipated resulting contract start date is July 1, 2026.
 5. Contractor shall be responsible for any damages to any real or personal property provided by County beyond any reasonable or normal wear and tear.
 6. Contractor shall use the TFC dedicated telephone line and the telephone lines provided for Contractor co-located staff for the express purpose of handling County business calls. Contractor shall maintain a phone log containing a list of all long distance calls

made from the telephone lines funded by County, which will include the phone number, the person called, the name of the TFC participant for whom the call was made, and the purpose of the call. This list shall be submitted to County on a monthly basis.

B. County Responsibilities

County shall be responsible for all repairs and replacements related to the physical structure of the property and major appliances provided by County, including but not limited to:

1. Windows, window screens, and doors
2. Walls, ceilings, and flooring
3. Plumbing, electrical, and heating, ventilation, and air conditioning systems
4. Major appliances, such as stove, oven, refrigerator, and dishwasher

C. Contractor Responsibilities

Contractor shall be responsible for the repair or replacement of all residential and community furniture and furnishings and minor appliances provided for use by Foster Youth/NMDs, including but not limited to:

1. Beds, mattresses, dressers, and closets
2. Couches, chairs, and dining tables
3. Outdoor furniture and decor
4. Minor appliances, such as televisions, microwaves, and toasters

D. Repair Request Turnaround

County shall make reasonable efforts to complete repairs to County-owned property within 72 hours of receiving a written repair request from Contractor, except in cases requiring specialized parts or services, in which case County shall provide an estimated completion timeline.

8. RECORDS

A. Foster Youth/NMD Records

1. Contractor shall prepare and maintain accurate and complete written records of each Foster Youth/NMD served in a form acceptable to County. Documentation containing confidential mental health information is to be retained and securely stored in the Foster Youth/NMD's clinical case file in compliance with CDHCS and Medi-Cal standards.
2. In addition to the records required to be maintained by Title 22, CCR, Contractor shall also maintain the following information in Foster Youth/NMD's case files:
 - a. Information regarding the Foster Youth/NMDs participation in TPSP/ILP services as applicable;
 - b. Statement of behaviors with potential risk and/or safety concerns;
 - c. Interagency Placement Committee referral for STRTP Placement and/or Admission Statement;

- d. Initial and monthly CFT reports;
 - e. Foster Youth/NMD's financial information, including disbursements for clothing and property signed for by Foster Youth/NMD, and allowances received by, and signed for, by Foster Youth/NMD;
 - f. Intake interviews conducted with Foster Youth/NMDs;
 - g. Special Incident Report;
 - h. Written quarterly evaluations;
 - i. CANS assessment and/or other mental health assessments;
 - j. Mental health treatment plan and mental health program progress notes;
 - k. HEP Encounter Forms;
 - l. Records of medical/dental visits and treatment, including a copy of physical or its equivalent that is less than one year old;
 - m. Foster Youth/NMD's monthly weight chart;
 - n. Psychotropic medication orders/prescriptions and forms regarding psychotropic medication, including, but not limited to, JV-220, JV-220(A), JV-220(B), and court approved JV-223;
 - o. Monthly feedback from the Foster Youth/NMD's school regarding academic and social performance; and
 - p. Foster Youth's most current IEP.
- B. House Log Book**
1. Contractor shall maintain a House Log Book in each STRTP TFC home that is handwritten, reviewed, and initialed at the beginning of each work shift, with entries made subsequent to the last working shift. The House Log Book shall be maintained with a chronological daily record of the following:
 - a. Population count;
 - b. Visitors; Special incidents/problems; Restraints and law enforcement contacts;
 - c. Group and individual activities, including participants in therapeutic treatment, length of time of therapeutic treatment activities;
 - d. Significant reactions, including, but not limited to, emotional outbursts, aggressive or violent behaviors, and/or self-injurious behaviors of Foster Youth/NMD, to telephone calls when such are openly displayed;
 - e. Furloughs or other off-site trips of Foster Youth/NMD; and
 - f. Contractor staff on duty, including date and time staff enters and leaves the home.
 2. At the beginning of each working shift, Contractor's staff shall individually review and initial all House Log Book entries made subsequent to their last working shift.
- C. Visitors Log Book**

1. Each STRTP TFC home shall maintain a separate Visitor Sign-In/Sign-Out Log which shall be retained by Contractor for a minimum of five years from date of final payment under this Contract or until all pending County, State and federal audits are completed, whichever is later.

9. REPORTING REQUIREMENTS

Contractor shall maintain records, collect data, and provide reports related to the services provided as mandated by County, State, and Federal Governments. Reporting requirements shall include all reports and data collection that is required to track and report progress on goals, strategies, and outcome objectives as stated in Paragraph 3 of this Scope of Work. County may modify the provisions of this Paragraph upon written notice to Contractor. Reports shall include, but not limited to, the following:

A. Needs and Services Plan (NSP)

1. The NSP shall be developed by Contractor in partnership with all of the Foster Youth/NMD's treatment providers, including Contractor's treatment staff, County Social Worker, and Foster Youth/NMD's family as appropriate, within the first 30 days of placement.
2. Contractor shall place a copy of the NSP, signed by all applicable parties, in the Foster Youth's/NMD's file.
3. Contractor shall provide a signed electronic or hard copy of the NSP to the Foster Youth's/NMD's Social Worker/Probation Officer within seven calendar days of completion.
4. The NSP shall identify the Foster Youth's/NMD's strengths and progress, including specific steps needed for Foster Youth/NMD to move to Lower Level of Care of a family setting.
5. The NSP shall be based on information specified in ILS Section 87070, in compliance with ILS 87068.2 and 87068.22.
6. Contractor shall review, update, and submit the NSP with signatures to County monthly, unless otherwise specified. The monthly review may be conducted at Contractor's facility with Foster Youth's/NMD's Social Worker/Probation Officer and Contractor.
7. All approvals for the Foster Youth/NMD to be off-site unsupervised, shall be written into the Foster Youth/NMD's NSP and signed and approved by the Foster Youth/NMD's County Social Worker/Probation Officer prior to leave.
8. All approvals for Foster Youth/NMD to serve restitution, have funding to be withheld for safety purposes, and/or have personal electronic devices withheld, shall be written into the NSP and signed and approved by the Foster Youth's/NMD's assigned Authorized Representative.

B. Mental Health Progress Notes

1. Mental health progress notes shall be completed daily, whenever there is a significant change in Foster Youth/NMD's condition or behaviors, or a significant event involving the Foster Youth/NMD occurs.
2. Mental health progress notes will be utilized to update the Foster Youth/NMD's NSP accordingly.

C. Quarterly Evaluation of Foster Youth/NMD

1. Contractor shall submit ongoing written evaluations on each Foster Youth/NMD to Foster Youth's/NMD's County Social Worker/Probation Officer on a quarterly basis, to be submitted within seven calendar days following the quarterly reporting period. These evaluations shall include, but not be limited to:
 - a. Updates for the Foster Youth/NMDs NSP as specified in Title 22 CCR, ILS Sections 87068.2 and 87068.22.
 - b. Progress toward accomplishing the goals, strategies, and outcome objectives described in Paragraph 3 of this Scope of Work.
 - c. Foster Youth's/NMD's progress toward accomplishing his/her long-range goal(s), short-term objectives, tasks, and placement in a family setting.
 - d. Identification of the Foster Youth's/NMD's areas of strength and concern.
 - e. Identification of service needs of the Foster Youth's/NMD's family and the plan for permanency.
 - f. Identification of Foster Youth's/NMD's unmet needs, and Contractor's recommendations and efforts made to meet these needs.
 - g. Updated assessment of Foster Youth's/NMD's adjustment/acclimation to Contractor's facility, program, peers, school, and staff.
 - h. Updated assessment of the Foster Youth's/NMD's progress towards transitional planning/independent living goals, if applicable.
 - i. Current status of Foster Youth's/NMD's physical and psychological health, and a report of medical and mental health care received, and medication(s) administered.
 - j. Modification of the treatment plan, anticipated length of placement, and any barriers to permanency.
 - k. A record of any serious behavioral problems and how these problems were treated, as well as the Foster Youth's/NMD's response to treatment.
 - l. A record of parental contacts, conferences and visits; contacts with relatives, friends, and significant others, so far as they are made known, other FFE efforts, and any significant reactions thereto openly displayed by Foster Youth/NMD.
 - m. The dates of contacts with Foster Youth's/NMD's Social Worker/Probation Officer during the quarter. This part of the report shall include the number of visits to Foster Youth/NMD, as well as phone calls placed and received.
 - n. The dates of contacts with substance abuse treatment professionals and other mental health professionals during the quarter.

- o. Summary of Foster Youth's/NMD's current educational progress.
2. Contractor shall also make available to Foster Youth's/NMD's County Social Worker/Probation Officer copies of any pertinent information utilized for the quarterly evaluation, including, school reports, medical reports, and psychological/psychiatric reports, as completed.

D. Semi-Annual Performance Outcomes Report

1. Contractor shall submit to RFA Program Manager, and SSA/CFS STRTP TFC Foster Care Liaison, a Semi-Annual Performance Outcomes Report in a format acceptable to County. Program Objectives and Performance Outcomes Measures shall be determined by County. Subject to 30 days advance written notice, County reserves the right to include or modify Program Objectives and Performance Outcomes Measures.
2. The Semi-Annual Performance Outcomes Report shall be submitted by the 10th calendar day of the month following each six month reporting cycle. The reporting cycles are January through June, and July through December.
3. Contractor shall report Program Objectives and Performance Outcomes Measures during each reporting cycle, including, but not limited to, the following:
 - a. Number of open beds at the beginning and end of each reporting cycle;
 - b. Number and gender of Foster Youth/NMDs placed in care during each reporting cycle;
 - c. Number of Foster Youth/NMDs served at the beginning, transitioned during, and at the end of the reporting cycle;
 - d. Age range of Foster Youth/NMDs served;
 - e. Number of placement admissions;
 - f. Number of Foster Youth/NMD discharged, including reason for discharge;
 - g. Upon discharge, the type of placement Foster Youth/NMD transitioned to and location; and
 - h. Breakdown of educational options utilized (i.e., school of origin, public school, non-public school, continuation/access schools, and adult education/college courses).
4. Provide to County a summary of all complaints and/or negative comments, as prescribed and in a format approved by County.

E. Monthly Report of Incidents

1. Contractor shall provide STRTP TFC Foster Care Liaisons and SSA Quality Assurance Department a monthly report of incidents of runaway episodes over 24 hours in length, Emergency Room visits, psychiatric hospitalization, and 911 calls. Monthly Report of Incidents shall be due by the first business day of the following month.

F. Unauthorized Absence Reports

1. An unauthorized absence is defined as an event when a Foster Youth's/NMD's whereabouts are unknown by Contractor's staff or when a Foster Youth/NMD has run away from placement.
2. In the case of an unauthorized absence, Contractor shall immediately telephone Foster Youth's/NMD's County Social Worker, Foster Youth's/NMD's Probation Officer when applicable, the local law enforcement agency, CCLD, and Foster Youth's/NMD's parents/guardians.
3. Contractor shall make direct person-to-person contact with the Social Worker/Probation Officer or their designee and provide written notification of the unauthorized absence within 24 hours of the absence to the Social Worker/Probation Officer.
4. Contractor shall submit the written incident report to Foster Youth's/NMD's Social Worker/Probation Officer within 24 hours of the absence via the Foster Youth Information Database (CFS) and (714) 935-7725 (Probation Department). Contractor shall submit a copy of this written report to the SSA STRTP Liaison, STRTP Program Manager, or designee, and Probation Department's STRTP Liaison/Probation Monitor.
5. If Foster Youth/NMD returns voluntarily, Contractor shall immediately notify the Foster Youth's/NMD's Social Worker/Probation Officer, STRTP Program Manager, the local law enforcement agency, CCLD, Foster Youth's/NMD's parents/guardians and, as appropriate, the Foster Youth's/NMD's mental health and/or physical health provider.
6. Following the Foster Youth's/NMD's return, Contractor shall provide an evaluation for Foster Youth/NMD emphasizing the significance of their absence and appropriate follow-up intervention. Discussions resulting from the evaluation shall be documented in Foster Youth's/NMD's record and information provided to the Foster Youth's/NMD's Social Worker/Probation Officer.
7. In the event of an unauthorized absence, Contractor shall notify County's designee, as outlined in Subparagraph 9.F.2 of this Scope of Work. Contractor agrees to return the Foster Youth/NMD to Contractor's care, except under the following circumstances:
 - a. Contractor and County agree there is an imminent safety risk for the Foster Youth/NMD or the program should he/she/they be returned.
 - b. Contractor has been notified that the bed has been closed, at the discretion of County.
 - c. The Foster Youth/NMD has exceeded the duration of County's authorized bed hold or was absent more than 14 cumulative days within the month.
8. In the event that a 14 day placement change notice has been requested by Contractor and the Foster Youth/NMD returns within the 14 day period and the bed has not been closed, Contractor agrees to return the Foster Youth/NMD to Contractor's care until a CFT meeting can be facilitated.
9. If the Foster Youth/NMD has not returned prior to the completion of the 14 day notice period, Contractor is not obligated to take the Foster Youth/NMD back to the facility

and the bed will be closed. County will then assume responsibility for securing alternative placement arrangements for the Foster Youth/NMD.

10. Contractor shall participate in a CFT meeting upon the request of County when the Foster Youth/NMD returns, to provide information relevant to determining appropriate placement options.
11. Contractor shall maintain records of unauthorized absences in Foster Youth's/NMD's record.
12. Contractor shall maintain and secure Foster Youth's/NMD's possessions in the event of an unauthorized absence.

G. Special or Unplanned Incident Reports

1. Serious Illness, Accident/Injury, or Death

- a. Contractor shall immediately telephone County Social Worker, or official designee in case of their absence, and Probation Officer, if the Foster Youth/NMD has one, or official designee in case of their absence, and make direct person-to-person contact upon becoming aware of any serious illness, accident/injury, hospitalization, or death of a Foster Youth/NMD in Contractor's care. If the Social Worker or designees are unavailable, Contractor shall notify Orangewood Children and Family Center (OCFC) Intake Services at (714) 935-7080. In the event Probation Officer or designees are unavailable, Contractor shall notify Custody Intake at (714) 935-7632. In the case of death, Contractor shall also notify local law enforcement. Contractor shall follow the verbal report with the submission of an electronic Special Incident Report via the online FYI system within one business day of such serious illness, accident/injury, hospitalization, or death occurs. In the event the FYI system is not available, Contractor shall submit the Special Incident Report via facsimile within one business day of the incident to avoid delay. Standard protocol shall resume once the FYI system becomes available. Contractor shall provide Probation Officer a written report or via electronic/facsimile for incidents involving placements for Probation Department. The verbal and electronic/facsimile reports shall include, but not be limited to:
 - i. Name of the Foster Youth/NMD;
 - ii. Date of serious illness, accident/injury or death;
 - iii. Nature of the illness/injury or the circumstances of the death;
 - iv. Name or names of Contractor's officers, employees or agents with knowledge of the event;
 - v. Name of the attending physician;
 - vi. Name of the hospital; and
 - vii. When applicable, the police report number, name of the police agency handling the incident, date of the police report, Foster Youth's race and ethnicity, and a summary of the circumstances.

H. Other Special Incidents

1. Contractor shall immediately telephone the Foster Youth's/NMD's County Social Worker, or designee, and Probation Officer, if the Foster Youth/NMD has one, and make contact if any of the following occurs:
 - a. Assault or verbal threats to staff, other youth, or community at large;
 - b. Medication errors, including mis-administered medication(s) and missed medication(s);
 - c. Foster Youth/NMD refused medication;
 - d. Accident/Minor injury;
 - e. Self-injury;
 - f. Sexual activity;
 - g. Suspension from school;
 - h. Unauthorized school absences;
 - i. Contraband of illegal substance and/or weapons;
 - j. Law enforcement intervention and/or arrest;
 - k. Property damage and or vandalism;
 - l. Personal rights complaint; and
 - m. Any behavior or activities by any Contractor's volunteers or personnel while on duty which substantially disrupts activities within Contractor's facility and jeopardizes the status, safety, or health of a Foster Youth/NMD placed by County.
2. County may, at his/her sole discretion, add, delete, waive, or otherwise modify individual reporting requirements as stated in Paragraph 9 of this Scope of Work.

I. Transition Determination Plan

1. Contractor shall submit a written closing summary report within five calendar days prior to Foster Youth/NMD transitioning from STRTP, as outlined in CDSS/CCLD ILS STRTP Regulations, to Foster Youth/NMD's assigned County Social Worker and/or Probation Officer. The Transition Determination Plan shall include, but not be limited to:
 - a. Records of monies (i.e., savings) owed to the Foster Youth/NMD upon discharge; and
 - b. An inventory of Foster Youth/NMD's personal property and clothing released to Foster Youth/NMD.
2. Upon Foster Youth/NMD's discharge, Contractor shall provide the assigned Social Worker/Probation Officer written documentation of Foster Youth's/NMD's medical and dental appointments, and follow-up care, including all medication that was prescribed to the Foster Youth/NMD.

J. Handling Complaints

Contractor shall:

1. Develop, operate, and maintain procedures for receiving, investigating, and responding to complaints, including Civil Rights complaints, requests for County reviews, negative comments, and other complaints relating to the STRTP TFC filed by Foster Youth/NMDs, other contract service providers, community organizations, and the public.
2. Maintain a log of complaints and responses to complaints.
3. Institute a system of follow-through when complaints cannot be resolved informally, which adheres to formal plans for specific actions and strict time deadlines.
4. Respond to complaints within two business days.
5. Refer to Paragraph 10 of the Contract when addressing Civil Rights complaints.
6. Identify issues with potential legal implications and review any such cases with designated County staff prior to responding to the complaints.
7. Provide to County, in a form approved by County, information pertaining to complaints, including County's response, as described in Subparagraph 9.J of this Scope of Work, within 10 business days of the complaint.

10. MEETING REQUIREMENTS

Contractor shall:

- A. Participate in service delivery meetings on a monthly basis, or as requested by SSA.
- B. Attend MDT meetings to engage Client(s)/Families in a discussion focused on Client(s)/Families' strengths and priority needs.
- C. Attend Advisory Board Meetings. CFS representative(s) shall meet monthly with Contractor's Family Consultants to provide consultation and assistance in monitoring, and determining the programmatic services provided under this Contract. The assigned social worker of the particular case(s) to be discussed during the meeting shall be notified by Contractor and given an opportunity to participate.
- D. Attend Contractors' Forum Meeting. Contractor's Program Coordinator and Assistant Coordinator must attend bimonthly Contractors' Forum meeting.

11. UTILIZATION REVIEW

- A. Contractor and County's designee shall meet at least annually to review and evaluate a random selection of Foster Youth/NMD records. The review may include, but is not limited to, an evaluation of the necessity and appropriateness of services provided and length of services. Cases to be reviewed shall be randomly selected by County and may include both open and closed cases.
- B. County may conduct a Utilization Review (UR) at Contractor's facility referenced in this Scope of Work, with date and time determined at County's discretion. County 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.

- C. In the event Contractor, County and County’s CFS staff representatives and/or County’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 the Termination clauses of this Contract.

12. STAFFING REQUIREMENTS

- A. Contractor shall remain in compliance with all STRTP Personnel Requirements per ILS 87065 et seq and Plan of Operation/Program Statement.
- B. Contractor shall provide access to nursing services 24 hours a day, seven days per week and meets the criteria of the STRTP ILS Section 87089.2.
- C. Same gender supervision during overnight shifts is a best practice. To the extent allowable under the law, Contractor shall use best efforts to staff overnight shifts with same gender staff members, whenever possible; thereby during overnight shifts using only female staff members in the female STRTP TFC home and only male staff members in the male STRTP TFC home.
- D. All direct services must be linguistically and culturally responsive to the Foster Youth/NMDs and their involved family members served. Although English is the predominant language spoken, there are Foster Youth/NMDs whose primary language is not English (e.g., Spanish or Vietnamese).
- E. Volunteers
 - 1. Contractor will indicate the use of volunteers in their Plan of Operation/Program Statement and adhere to the requirements of ILS Sections 87065 and 87065.1. Plan of Operation/Program Statement will include the following:
 - a. Type and degree of supervision provided; and
 - b. Description of the duties to be performed by volunteers.
- F. Contractor staff shall appear and testify at Juvenile Court hearings, as requested by SSA.
- G. Contractor shall notify County within 10 calendar days of any staff changes, including, but not limited to, changes in Facility Administrator, Head of Service, and/or unexpected changes in Foster Youth/NMD’s Mental Health Clinician that could impact Foster Youth/NMD’s therapeutic treatment.
- H. Contractor’s Employee Records
 - 1. Contractor shall maintain and retain records on each employee and volunteer as required by Title 22 CCR, Section 80066 and ILS Section 87066. Such records shall include, but not be limited to:
 - a. A completed and signed criminal record statement;
 - b. Proof of automobile insurance;
 - c. Completed reference checks;
 - d. Health questionnaire;

- e. Department of Motor Vehicle (DMV) driving record printout, including copy of valid California Driver’s License, if transporting Foster Youth/NMDs;
- f. Confidentiality agreement;
- g. Child abuse/elder abuse reporting requirements;
- h. Education credentials; Annual training completed;
- i. Disciplinary actions taken, if applicable; and
- j. Documentation of all in-service training content, and attendance for staff involved in direct service contact with Foster Youth/NMDs.

13. TRAINING

- A. Contractor shall maintain compliance with requirements for personnel training pursuant to ILS Sections 87065.1 and 87095.65, and any additional training determined to be mandatory by County, including, but not limited to, annual Child Abuse and Dependent/Elder Abuse Reporting trainings and trainings held at STRTP Forums. Contractor shall conduct subsequent training(s) for its staff, and shall:
 - 1. Provide ongoing staff training and assistance to ensure that all assignments are effectively handled;
 - 2. Ensure all staff complete special medical care training when deemed necessary, to facilitate placement and supervision of Foster Youth/NMDs with specified medical conditions; and
 - 3. Ensure that staff participate in trainings related to the Health Insurance Portability and Accountability Act and confidentiality.

14. QUALITY ASSURANCE/QUALITY CONTROL

- A. Contractor shall develop and utilize a comprehensive continuous quality improvement (CQI) plan in accordance with ILS Section 87081, to monitor the level of program service and quality.
- B. Contractor shall submit to County a copy of any new or revised CQI plan upon Contract start date and when changes occur.

15. COUNTY RESPONSIBILITIES

County shall:

- A. Provide consultation and technical assistance and will monitor performance of Contractor in meeting the terms of the resulting Contract, as permitted by CCLD.
- B. Provide assistance with emergencies. Emergency after hours telephone numbers are:

SSA/Orangewood Children and Family Center:
(714) 935-7171

Probation Department/Juvenile Hall:
(714) 935-6660

16. OUTSIDE CONTACTS

Contractor shall:

- A. Immediately inform County upon receiving any inquiry from an elected official, their representative, Foster Youth/NMD advocate, or the press, and immediately provide information in order to permit County to respond.
- B. Consult with County prior to initiating and/or responding to contact with a Foster Youth/NMD advocate or the press.
- C. Consult with County prior to initiating and/or responding to contact with an Orange County elected official or their representative.

ATTACHMENT B - INFORMATION TECHNOLOGY SECURITY PROVISIONS

1. Contractor's Policies, Procedures, and Technical, Physical, and Administrative Safeguards:

All Contractors with access to County data and/or systems shall establish and maintain policies, procedures, and technical, physical, and administrative safeguards designed to:

- A. 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,
- B. Protect against any threats or hazards to the security or integrity of County data, systems, or other confidential information,
- C. Protect against unauthorized access, use, or disclosure of personal or County confidential information,
- D. Maintain reasonable procedures to prevent, detect, respond, and provide notification to the County regarding any internal or external security breaches,
- E. 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
- F. 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.

2. County of Orange Information Technology Security Provisions Document:

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

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

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.

3. Contractor's Information Security Program:

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.

4. Information Access:

- A. 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.
- B. 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.
- C. 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.
- D. 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.

5. Data Security Requirements:

- A. 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).
- B. 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.
- C. 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.
- D. 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.
- E. 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.

6. 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.

7. General Security Standards:

Contractor will be solely responsible for the information technology infrastructure, including all computers, software, databases, electronic systems (including database management systems, email systems, auditing, and monitoring systems) and networks used by or for Contractor (“Contractor Systems”) to access County resources (including County systems), County data or otherwise in connection with the Services and shall prevent unauthorized access to County resources (including County systems) or County data through the Contractor Systems.

- A. **Contractor System(s) and Security:** At all times during the contract term, Contractor shall maintain a level of security with regard to the Contractor Systems, that in all events is at least as secure as the levels of security that are common and prevalent in the industry and in accordance with industry best practices (NIST 800-53). Contractor shall maintain all appropriate administrative, physical, technical, and procedural safeguards to secure County data from data breach, protect County data and the Services from loss, corruption, unauthorized disclosure, and from hacks, and the introduction of viruses, disabling devices, malware, and other forms of malicious and inadvertent acts that can disrupt County’s access and use of County data and the Services.

- B. **Contractor and the use of Email:** Contractor, including Contractor’s employees and subcontractors, that are provided a County email address must only use the County email system for correspondence of County business. Contractor, including Contractor’s employees and subcontractors, must not access or use personal, non-County Internet (external) email systems from County networks and/or County computing devices. If at any time Contractor’s performance under this Contract requires such access or use, Contractor must submit a written request to County with justification for access or use of personal, non-County Internet (external) email systems from County networks and/or computing devices and obtain County’s express prior written approval.

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

8. 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.

9. Security Breach Notification:

- A. 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).
- B. 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.
- C. 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 12 months following the date of notification to such individuals.
- D. Contractor shall indemnify, defend with counsel approved in writing by County, and hold County and County Indemnitees harmless from and against any and all claims, including reasonable attorney's fees, costs, and expenses incidental thereto, which may be suffered

by, accrued against, charged to, or recoverable from County in connection with the occurrence.

Notification shall be sent to:

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

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

10. Security Audits:

- A. 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).
- B. 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 60 calendar days of such audit or assessment. Contractor will provide a copy of the audit report to County within 30 days after Contractor's receipt of request for such report(s).
- C. 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.
- D. 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

11. Business Continuity and Disaster Recovery (BCDR):

- A. 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.
- B. 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 four hours, and every effort shall be undertaken to restore contracted services, data, operations, security, and functionality.
- C. All data and/or systems and technology provided by the Contractor internally and through third-party vendors shall have resiliency and redundancy capabilities to achieve high availability and data recoverability. Contractor Systems shall be designed, where practical and possible, to ensure continuity of service(s) in the event of a disruption or outage.

ATTACHMENT C - INFORMATION TECHNOLOGY SECURITY GUIDELINES

All contractors who contract with the County of Orange ("County") shall work cooperatively to assist County in achieving the objectives and abide by the applicable terms under these Guidelines for all Controls one (1) thru six (6) below at all times during the term of its contract with County.

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.

A. GOALS AND OBJECTIVES

1. Services are identified and prioritized.
2. Assets are inventoried, and the authority and responsibility for these assets is established.
3. The relationship between assets and the services they support is established.
4. The asset inventory is managed.
5. Access to assets is managed.
6. Information assets are categorized and managed to ensure the sustainment and protection of the critical service.
7. Facility assets supporting the critical service are prioritized and managed.

B. ASSET MANAGEMENT POLICY STATEMENTS

1. Services Inventory

- a. Departments and/or contractors shall maintain an inventory of its services. This listing shall be used by the department to assist with its risk management analysis.

2. Asset Inventory – Information

- a. 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.
- b. 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.

- c. Departments and/or contractors shall establish internal procedures for the secure handling and storage of all electronically-maintained County information that is owned or controlled by the department.

3. Asset Inventory - Technology (Devices, Software)

- a. 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:
 - i. Desktop computers,
 - ii. Laptop Computers,
 - iii. Tablets (iPads and Android devices),
 - iv. Mobile Phones (basic cell phones),
 - v. Smart Phones (iPhones, Blackberry, Windows Phones and Android Phones),
 - vi. Servers,
 - vii. Storage devices,
 - viii. Network switches,
 - ix. Routers,
 - x. Firewalls,
 - xi. Security Appliances,
 - xii. Internet of Things (IoT) devices,
 - xiii. Printers,
 - xiv. Scanners,
 - xv. Kiosks and Thin clients,
 - xvi. Mainframe Hardware, and
 - xvii. VoIP Phones.
- b. Asset inventory shall map assets to the services they support.
- c. Departments and/or contractors shall adopt a standard naming convention for devices (naming convention to be utilized as devices are serviced or purchased).
- d. Each department and/or contractor 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.

4. Asset Inventory - Facilities

- a. Departments and/or contractors shall maintain an inventory of its facilities. This listing shall be used by the department to assist with its risk management analysis.
- b. Departments and/or contractors shall identify the facilities used by its critical services.

5. Access Controls

- a. Departments and/or contractors shall establish a procedure that ensures only users with legitimate business needs to access County IT resources are provided with user accounts.
- b. 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.
- c. 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.
- d. The owner of each County system, or their designee, provides written authorization for all internal and external user access.
- e. 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.
- f. All County workforce members are to be assigned a unique user ID to access the network, as applicable.
- g. 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.
- h. User accounts shall not be shared with others including, but not limited to, someone whose access has been denied or terminated.
- i. Departments and/or contractors 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.

6. Asset Sanitation/Disposal

- a. Unless approved by County management, no County computer equipment shall be removed from the premises.
- b. Prior to re-deployment, storage media shall be appropriately cleansed to prevent unauthorized exposure of data.

- c. Surplus, donation, disposal or destruction of equipment containing storage media shall be appropriately disposed according to the terms of the equipment disposal services contract.
- d. Sanitization methods for media containing County information shall be in accordance with NSA (National Security Agency) standards (for example, clearing, purging, or destroying).
- e. 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.

A. GOALS AND OBJECTIVES

- 1. Control objectives are established.
- 2. Controls are implemented.
- 3. Control designs are analyzed to ensure they satisfy control objectives.
- 4. Internal control system is assessed to ensure control objectives are met.

B. CONTROL MANAGEMENT POLICY STATEMENTS

1. Physical and Environmental Security

- a. 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.
- b. 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.
- c. Physical protection measures against damage from external and environmental threats shall be implemented by all departments as appropriate.
- d. Access to any office, computer room, or work area that contains sensitive information shall be physically restricted from unauthorized access.
- e. 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.

- f. Continuity of power shall be provided to maintain the availability of critical equipment and information systems.
- g. 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.
- h. Equipment shall be properly maintained to ensure its continued availability and integrity.
- i. All shared IT infrastructure by more than one department shall meet countywide security policy for facility standards, availability, access, data & network security.

2. Network Segmentation

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

- a. 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.
- b. Segment the network into multiple, separate zones based on the devices (servers, workstations, mobile devices, printers, etc.) connected to the network.
- c. Create separate network segments (e.g., VLANs) for BYOD (bring your own device) systems or other untrusted devices.
- d. 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.

3. Mobile Computing Devices

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

- a. Establish and manage a process for authorizing, issuing and tracking the use of MCDs.
- b. Permit only authorized MCDs to connect to County information assets or networks that store, process, transmit, or connects to County information and information assets.
- c. Implement applicable access control requirements in accordance with this guideline, such as the enforcement of a system or device lockout after 15 minutes of inactivity requiring re-entering of a password to unlock.
- d. Install an encryption algorithm that meets or exceeds industry recommended encryption standard for any MCD that will be used to store County information.

- e. Ensure that MCDs are configured to restrict the user from circumventing the authentication process.
- f. Provide security awareness training to County employees that informs MCD users regarding MCD restrictions.
- g. Label MCDs with County address and/or phone number so that the device can be returned to the County if recovered.
- h. 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.

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.

- a. 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.
- b. The County authorizes the use of personal devices to access resources that do not traverse the County network directly. Such resources include County's SaaS applications. 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.
- c. The County will respect the privacy of a user's voluntary use of a personally owned device to access County IT resources.
- d. 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.

5. **Logon Banners and Warning Notices**

- a. At the time of network login, the user shall be presented with a login banner.
- b. 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.
- c. Warning banners shall remain on the screen until the user takes explicit actions to log on to the information system.
- d. 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.

- e. At a minimum, banner messages shall provide appropriate privacy and security information and shall contain information informing potential users that:
 - i. User is accessing a government information system for conditions of use consistent with state and federal information security and privacy protection laws.
 - ii. System usage may be monitored, recorded, and subject to audit.
 - iii. Unauthorized use of the system is prohibited and subject to criminal and civil penalties.
 - iv. Use of the system indicates consent to monitoring and recording.

6. Authentication

- a. Authenticate user identities at initial connection to County resources.
- b. Authentication mechanisms shall be appropriate to the sensitivity of the information contained.
- c. Users shall not receive detailed feedback from the authenticating system on failed logon attempts.

7. Passwords

- a. County approved password standards and/or guidelines shall be applied to access County systems. These standards extend to mobile devices and personally owned devices used for work.
- b. 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:
 - i. Passwords will contain a minimum of one (1) upper case letter
 - ii. Passwords will contain a minimum of one (1) lower case letter
 - iii. Passwords will contain a minimum of one (1) number: 1- 0
 - iv. Passwords will contain a minimum of one (1) special character: !, @, #, \$, %, ^, &, *, (,)
 - v. Password characters will not be sequential (Do not use: ABCD , This is ok: ACDB)
 - vi. Password characters will not be repeated in a row (Do not use: P@\$\$\$. This is ok: P@\$\$S)
 - vii. COMPLEX PASSWORD EXAMPLE: P@\$SWoRd13
 - viii. Passphrases example: The\$kyIsBlue2day
 - ix. Passwords cannot contain the user's full name or network login.

- c. Passwords shall have a minimum length of twelve (12) characters.
- d. Passwords shall not be reused for twelve (12) iterations.
- e. Departments and/or contractors 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.
- f. 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.
- g. Newly created accounts shall be assigned a randomly generated password prior to account information being provided to the user.
- h. 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.
- i. 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.
- j. 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.
- k. All passwords are to be treated as sensitive information.
- l. 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.
- m. 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.

C. Inactivity Timeout and Restricted Connection Times

1. Automatic lockouts for system devices, including workstations and mobile computing devices, after no more than 15 minutes of inactivity.
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.

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

D. Account Monitoring

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. The control mechanisms for all types of access to County IT resources by contractors, customers or vendors are to be documented.
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.
4. After a longer period, such as 60 days, the account shall be disabled by the system when the technology is feasible or available.
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.

E. Administrative Privileges

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. Administrative accounts shall only be granted to individuals who have a job requirement to conduct systems administration tasks.
3. Administrative accounts shall be requested in writing and must be approved by the Department Head or designated representative using the Security Review and Approval Process.
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.
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.
6. All passwords for privileged system-level accounts (e.g., root, enable, OS admin, application administration accounts, etc.) shall comply with Controls Management B.7.

F. Remote Access

1. Departments and/or contractors 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. Remote access privileges shall be granted to County workforce members only for legitimate business needs and with the specific approval of department management.
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 the County. 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.
4. Remote sessions shall be terminated after 15 minutes of inactivity requiring the user to authenticate again to access County resources.
5. All remote access infrastructures shall include the capability to monitor and record a detailed audit trail of each remote access attempt.
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.
7. Periodic assessments shall be performed to identify unauthorized remote connections. Results shall be used to address any vulnerabilities and prioritized according to criticality.
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.
9. Users attempting to use external remote access shall utilize a County-approved multi-factor authentication process.
10. All remote access implementations that involve non-County infrastructures shall be reviewed and approved by both the department and the County. This approval shall be received prior to the start of such implementation.
11. Remote access privileges to County IT resources shall not be given to contractors and customers 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.

G. Wireless Access

1. Departments and/or contractors 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. Only wireless systems that have been evaluated for security by both department management and the County shall be approved for connectivity to County networks.
3. County data that is transmitted over any wireless network shall be protected in accordance with the sensitivity of the information.
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.
5. Each department and/or contractor 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.

H. System and Network Operations Management

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

I. System Monitoring and Logging

1. Systems operational staff shall maintain appropriate log(s) of activities, exceptions and information security events involving County information systems and services.
2. Each department and/or contractor shall maintain a log of all faults involving County information systems and services.
3. Logs shall be protected from unauthorized access or modifications wherever they reside.
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.
5. Auditing and logging of user activity shall be implemented on all critical County systems that support user access capabilities.
6. Periodic log reviews of user access and privileges shall be performed in order to monitor access of sensitive information.

J. Malware Defenses

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, antispymware, 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. Special features designed to filter out malicious software contained in either email messages or email attachments shall be implemented on all County email systems.
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.

K. Data Loss Prevention

1. Departments and/or contractor shall implement host-based Data Loss Prevention (DLP) to reduce the risk of data breach related to sensitive information.
2. Departments and/or contractors shall deploy encryption software on mobile devices containing sensitive.

L. Data Transfer

1. Agreements shall be implemented for the exchange of information between the County and other entities. As well as between departments.
2. County information accessed via electronic commerce shall have security controls implemented based on the assessed risk.

M. Encryption

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. 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.
3. Where appropriate, encryption shall be used to protect confidential application data that is transmitted over open, untrusted networks, such as the Internet.
4. When cryptographic controls are used, procedures addressing the following areas shall be established by each department:
 - a. Determination of the level of cryptographic controls
 - b. Key management/distribution steps and responsibilities
5. Encryption keys shall be exchanged only using secure methods of communication.

N. System Acquisition and Development

1. Departments and/or contractors 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) for critical rating (RTO) and continuity purposes.
2. An application owner shall be designated for each internal department business application.
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 1.2.5: Access Controls.
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 guideline.
5. In situations where data needs to be isolated because there would be a conflict of interest, data security shall be designed and implemented to ensure that isolation.

O. Business Requirements

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

P. System Files

1. Operating system files, application software and data shall be secured from unauthorized use or access.
2. 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.
3. System tests shall be performed on data that is constructed specifically for that purpose.
4. System testing shall not be performed on operational data unless the necessary safeguards are in place.
5. 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.

Q. System Development & Maintenance

1. 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. 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.
3. 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.
4. Systems shall be hardened, and logs monitored to ensure the avoidance of the introduction and exploitation of malicious code.
5. All County workforce members, including contractors, 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.
6. In conjunction with other access control policies, any opportunity for information leakage shall be prevented through good system design practices.
7. Departments and/or contractors are responsible for managing outsourced software development related to department-owned IT systems.

R. System Requirements

1. Any system that processes or stores County Information shall:
 - a. Baseline configuration shall incorporate Principle of Least Privilege and Functionality.
 - b. Systems shall be deployed where feasible to utilize existing County authentication methods.
 - c. Session inactivity timeouts shall be implemented for all access into and from County networks.
 - d. All applications are to have access controls unless specifically designated as a public access resource.
 - e. Meet the password requirements defined in Section 2.2.7: Passwords.
 - f. Strictly control access enabling only privileged users or supervisors to override system controls or the capability of bypassing data validation or editing problems.
 - g. Monitor special privilege access, e.g. administration accounts.
 - h. Restrict authority to change master files to persons independent of the data processing function.

- i. 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.
- j. Be capable of routinely monitoring the access to automated systems containing County Information.
- k. Log all modifications to the system files.
- l. Limit access to system utility programs to necessary individuals with specific designation.
- m. Delete or disable all default accounts.
- n. 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.
- o. Restrict access to server-file-system controls that allow access to other users' files.
- p. Ensure that servers containing user credentials shall be physically protected, hardened and monitored to prevent inappropriate use.

S. Procurement Controls

- 1. Breach notification requirements clause to be included in new or renewal contracts for systems containing sensitive information.
- 2. 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 subcontractor's systems involving County's data.
- 3. 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 contractors are aware of and are in compliance with County's cybersecurity policies, if applicable. Departments shall obtain documentation supporting the business partners, contractors, or consultants' compliance with County's cybersecurity policies such as:
 - a. SOC 1 Type 2
 - b. SOC 2 Type 2
 - c. Security Certifications (ISO, PCI, etc.)
 - d. FedRAMP certification
 - e. Penetration Test Results

T. IT Services Provided to Public

- 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.

U. Removable Media

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:

- A. Application and system security
- B. Configuration management
- C. Change control procedures
- D. Encryption and key management
- E. 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.

A. GOALS AND OBJECTIVES

1. The lifecycle of assets is managed.
2. The integrity of technology and information assets is managed.
3. Asset configuration baselines are established.

B. CONFIGURATION & CHANGE MANAGEMENT POLICY STATEMENTS

1. Changes to all information processing facilities, systems, software, or procedures shall be strictly controlled according to formal change management procedures.
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 County in accordance with the County Security Review and Approval Process.
3. Only authorized users shall make any changes to system and/or software configuration files.

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.
5. Each department and/or contractor 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.
6. Each department and/or contractor shall conduct periodic audits designed to determine if unauthorized software has been installed on any of its computers.
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.
8. Production computing environments shall be separated from development and test computing environments to reduce the risk of one environment adversely affecting another.
9. System capacity requirements shall be monitored, and usage projected to ensure the continual availability of adequate processing power, bandwidth, and storage.
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.

A. GOALS AND OBJECTIVES

1. Preparation for vulnerability analysis and resolution activities is conducted.
2. A process for identifying and analyzing vulnerabilities is established and maintained.
3. Exposure to identified vulnerabilities is managed.
4. The root causes of vulnerabilities are addressed.

B. VULNERABILITY MANAGEMENT POLICY STATEMENTS

1. Departments and/or contractors 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 and/or contractor 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

A. GOALS AND OBJECTIVES

1. A process for identifying, analyzing, responding to, and learning from incidents is established.
2. A process for detecting, reporting, triaging, and analyzing events is established.
3. Incidents are declared and analyzed.
4. A process for responding to and recovering from incidents is established.
5. Post-incident lessons learned are translated into improvement strategies.

B. CYBERSECURITY INCIDENT MANAGEMENT POLICY STATEMENTS

1. Cybersecurity incident management procedures shall be established within each department and/or contractor 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:
 - a. System preparation
 - b. Problem identification
 - c. Problem containment
 - d. Problem eradication
 - e. Incident recovery
 - f. Lessons learned

2. The department shall act as the liaison between applicable parties during a cybersecurity incident. The department shall be the primary point of contact for all IT security issues.
3. A designated security contact for all cybersecurity incidents.
4. Departments and/or contractors 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. Departments and/or contractors shall develop and document procedures for reporting cybersecurity incidents. For example, all employees, contractors, 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.
6. Each department and/or contractor shall familiarize its employees on the use of its cybersecurity incident reporting procedures.
7. Contact with local authorities, including law enforcement, shall be conducted through an organized, repeatable process that is both well documented and communicated.
8. Contact with special interest groups, including media and labor relations, shall be conducted through an organized, repeatable process that is both well documented and communicated.
9. 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.
10. Departments shall report cybersecurity incidents to the County pursuant to the Contract.

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.

A. GOALS AND OBJECTIVES

1. Service continuity plans for high-value services are developed.
2. Service continuity plans are reviewed to resolve conflicts between plans.
3. Service continuity plans are tested to ensure they meet their stated objectives.
4. Service continuity plans are executed and reviewed.

B. SERVICE CONTINUITY MANAGEMENT POLICY STATEMENTS

1. Backups of all essential electronically maintained County business data shall be routinely created and properly stored to ensure prompt restoration.
2. Each department and/or contractor 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.
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.
4. Departments and/or contractors 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.

5. Backup media shall be labeled and handled in accordance with the highest sensitivity level of the information stored on the media.
6. Departments and/or contractors shall define and periodically test a formal procedure designed to verify the success of the backup process.
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.
8. Departments and/or contractors 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.
9. Alternate storage facilities shall be used to ensure confidentiality, integrity and availability of all County systems.
10. Each department and/or contractor shall develop, periodically update, and regularly test business continuity and disaster recovery plans in accordance with the County's Business Continuity Management Policy.
11. Departments and/or contractors shall review and update their Risk Assessments (RAs) and Business Impact Analyses (BIAs) as necessary, determined by department management (annually is recommended). 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.
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.
13. Each department and/or contractor 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.
14. Each department and/or contractor 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.

ATTACHMENT D - SSA STATE PRIVACY AND SECURITY PROVISIONS

DEFINITIONS

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

1. “**Assist in the administration of the Medi-Cal program**” means performing administrative functions on behalf of Medi-Cal programs, such as establishing eligibility, determining the amount of medical assistance, and collecting PII for such purposes, to the extent such activities are authorized by law.
2. “**Breach**” refers to actual loss, loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for other than authorized purposes have access or potential access to PII, whether electronic, paper, verbal, or recorded.
3. “**Contractor Worker**” means those Contractor employees, contractors, subcontractors, vendors and agents performing any functions for the Contractor that require access to and/or use of PII and that are authorized by the Contractor to access and use PII. An agent is a person or organization authorized to act on behalf of the Contractor.
4. “**PII**” includes “**Medi-Cal PII**” and is defined as personally identifiable information directly obtained in the course of performing an administrative function through the MEDS or IEVS systems on behalf of Medi-Cal programs that can be used alone, or in conjunction with any other information, to identify a specific individual. PII includes any information that can be used to search for or identify individuals, or can be used to access their files, including but not limited to name, social security number (SSN), date and place of birth (DOB), mother’s maiden name, driver's license number, or identification number. PII may also include any information that is linkable to an individual, such as medical, educational, financial, and employment information. PII may be electronic, paper, verbal, or recorded and includes statements made by, or attributed to, the individual.
5. “**Security Incident**” means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of PII, or interference with system operations in an information system which processes PII that is under the control of the County or California Statewide Automated Welfare System (CalSAWS) Consortium, or a contractor, subcontractor or vendor of the County.
6. “**Secure Areas**” means any area where:
 - A. Contractor Workers assist in the administration of Medi-Cal programs;
 - B. Contractor Workers use or disclose PII; or
 - C. PII is stored in paper or electronic format.
7. “**SSA-provided or verified data (SSA data)**” means:
 - A. Any information under the control of the Social Security Administration (SSA) provided to Department of Health Care Services (DHCS) and California Department of Social Services (CDSS) under the terms of an information exchange agreement with SSA (e.g., SSA provided date of death, SSA Title II or Title XVI benefit and eligibility data, or SSA citizenship verification); or

- B. Any information provided to the County of Orange by DHCS and CDSS, including a source other than SSA, but in which DHCS and CDSS attests that SSA verified it, or couples the information with data from SSA to certify the accuracy of it (e.g., SSN and associated SSA verification indicator displayed together on a screen, file, or report, or DOB and associated SSA verification indicator displayed together on a screen, file, or report).

AGREEMENTS

County of Orange and Contractor mutually agree as follows:

I. PRIVACY AND CONFIDENTIALITY

- A. Contractor Workers may use or disclose PII only as permitted in this Agreement and only to assist in the administration of Medi-Cal programs in accordance with Section 14100.2 of the Welfare and Institutions Code, Section 431.302 of Title 42 Code of Federal Regulations, as limited by this Agreement, and as otherwise required by law. Disclosures required by law or that are made with the explicit written authorization of the client, such as through an authorized release of information form, are allowable. Any other use or disclosure of PII requires the express approval in writing of County of Orange. No Contractor Worker shall duplicate, disseminate or disclose PII except as allowed in this Agreement.
- B. While County of Orange is a hybrid covered entity under the federal Health Insurance Portability and Accountability Act, as amended from time to time (HIPAA), the Contractor is not required to be the business associate of the County of Orange, if the activities of the Contractor are limited to determining eligibility for, or enrollment in, Medi-Cal programs (45 CFR 160.103). Nevertheless, it is the intention of the parties to protect the privacy and security of PII and the rights of Medi-Cal applicants and beneficiaries in a manner that is consistent with HIPAA and other laws that are applicable. It is not the intention of the parties to voluntarily subject the Contractor to federal HIPAA jurisdiction where it would not otherwise apply.
1. To the extent that other state and/or federal laws provide additional, stricter, and/or more protective (collectively, more protective) privacy and/or security protections to the PII covered under this Agreement beyond those provided through HIPAA, as applicable, Contractor shall:
 - a. Comply with the more protective of the privacy and security standards set forth in applicable state or federal laws to the extent such standards provide a greater degree of protection and security than HIPAA or are otherwise more favorable to the individuals whose information is concerned; and
 - b. Treat any violation of such additional and/or more protective standards as a breach or security incident, as appropriate, pursuant to Section VIII. of this Agreement. It is not the intention of the parties that this subsection I.B.(1)(b) expands the definitions of breach nor security incident set forth this Agreement unless the additional and/or more protective standard has a different definition for these terms, as applicable.

Examples of laws that provide additional and/or stricter privacy protections to certain types of PII include but are not limited to the Confidentiality of Alcohol and Drug Abuse Patient

Records, 42 CFR Part 2, Welfare and Institutions Code section 5328, and California Health and Safety Code section 11845.5.

- C. Access to PII shall be restricted to Contractor Workers who need to perform their official duties to assist in the administration of Medi-Cal programs.
- D. Contractor Workers who access, disclose or use PII in a manner or for a purpose not authorized by this Agreement may be subject to civil and criminal sanctions contained in applicable federal and state statutes.

II. PERSONNEL CONTROLS

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

- A. **Employee Training.** Train and use reasonable measures to ensure compliance with the requirements of this Agreement by Contractor Workers, including, but not limited to:
 1. Provide initial privacy and security awareness training to each new Contractor Worker within 30 days of employment;
 2. Thereafter, provide annual refresher training or reminders of the privacy and security safeguards in this Agreement to all Contractor Workers. Three or more security reminders per year are recommended;
 3. Maintain records indicating each Contractor Worker's name and the date on which the privacy and security awareness training was completed and;
 4. Retain training records for a period of five years after completion of the training.
- B. **Employee Discipline.**
 1. Provide documented sanction policies and procedures for Contractor Workers who fail to comply with privacy policies and procedures or any provisions of these requirements.
 2. Sanction policies and procedures shall include termination of employment when appropriate.
- C. **Confidentiality Statement.** Ensure that all Contractor Workers sign a confidentiality statement. The statement shall be signed by Contractor Workers prior to accessing PII and annually thereafter. Signatures may be physical or electronic. The signed statement shall be retained for a period of five years.

The statement shall include, at a minimum, a description of the following:

- 1. General Use of PII;
 - 2. Security and Privacy Safeguards for PII;
 - 3. Unacceptable Use of PII; and
 - 4. Enforcement Policies.
- D. **Background Screening.**
 1. Conduct a background screening of a Contractor Worker before they may access PII.
 2. The background screening should be commensurate with the risk and magnitude of harm the employee could cause. More thorough screening shall be done for those

employees who are authorized to bypass significant technical and operational security controls.

3. The Contractor shall retain each Contractor Worker's background screening documentation for a period of three years following conclusion of employment relationship.

III. MANAGEMENT OVERSIGHT AND MONITORING

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

- A. Conduct periodic privacy and security review of work activity by Contractor Workers, including random sampling of work product. Examples include, but are not limited to, access to case files or other activities related to the handling of PII.

The periodic privacy and security reviews shall be performed or overseen by management level personnel who are knowledgeable and experienced in the areas of privacy and information security in the administration of the Medi-Cal program and the use or disclosure of PII.

- B. Utilize Medi-Cal Eligibility Data System (MEDS) audit reports provided by the County of Orange and other system auditing tools available to Contractor to perform quality assurance and management oversight reviews of their Contractor Workers' access to Medi-Cal and SSA PII within data systems utilized, including MEDS. For additional information see [Medi-Cal Eligibility Division Information Letter | 21-34](#). Any instances of suspected security incidents or breaches are to be reported to the County of Orange immediately following the instructions within Section X of this Agreement.

To ensure a separation of duties, these system audit reviews shall be performed by privacy and security staff who do not have access to PII within the systems. DHCS requires the County of Orange to enforce a separation of duties, excluding any individual who uses MEDS to make benefit or entitlement determinations from participating in oversight, monitoring, or quality assurance functions. The County of Orange acknowledges that with smaller contractors the separation of duties requirement might create a hardship based on there being a small number of people available to perform various tasks. Requests for hardship exemptions will be approved on a case-by-case basis.

IV. INFORMATION SECURITY AND PRIVACY STAFFING

The Contractor agrees to:

- A. Designate information security and privacy officials who are accountable for compliance with these and all other applicable requirements stated in this Agreement.
- B. Provide the County of Orange with applicable contact information for these designated individuals using the County inbox listed in Section IX of this Agreement. Any changes to this information should be reported to the County of Orange within ten days.
- C. Assign Contractor Workers to be responsible for administration and monitoring of all security-related controls stated in this Agreement.

V. TECHNICAL SECURITY CONTROLS

The State of California Office of Information Security (OIS) and SSA have adopted the National Institute of Standards and Technology (NIST) Special Publication (SP) 800- 53, Security and Privacy controls for Information Systems and Organizations, and NIST SP 800-37, Risk Management Framework for Information Systems and Organizations.

OIS and SSA require organizations to comply and maintain the minimum standards outlined in NIST SP 800-53 when working with PII and SSA data. Contractor shall, at a minimum, implement an information security program that effectively manages risk in accordance with the Systems Security Standards and Requirements outlined in this Section of this Agreement.

Guidance regarding implementation of NIST SP 800-53 is available in the Statewide Information Management Manual (SIMM), SIMM-5300-A, which is hereby incorporated into this Agreement (Exhibit C) and available upon request.

[Remainder of page intentionally left blank]

A. Systems Security Standards and Requirements

1. Access Control (AC)

Control Number	AC-1
Title	Access Control Policy and Procedures
DHCS & CDSS Requirement	<p>The organization must:</p> <ul style="list-style-type: none"> a. Develop, document, and disseminate to designated organization officials: <ul style="list-style-type: none"> 1. An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; 2. Procedures to facilitate the implementation of the access control policy and associated access control controls; b. Review and update the current access control procedures with the organization-defined frequency.
Supplemental Guidance (from NIST 800-53)	<p>This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the AC family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.</p>
Control Number	AC-2
Title	Account Management
DHCS & CDSS Requirement	<p>The organization must:</p> <ul style="list-style-type: none"> a. Identify and select the accounts with access to PII to support organizational missions/business functions. b. Assign account managers for information system accounts; c. Establish conditions for group and role membership; d. Specify authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account; e. Require approvals by designated access authority for requests to create information system accounts; f. Create, enable, modify, disable, and remove information system accounts in accordance with organization account management procedures; g. Monitors the use of information system accounts;

	<ul style="list-style-type: none"> h. Notifies account managers when accounts are no longer required, when users are terminated or transferred; and when individual information system usage or need-to-know changes. i. Authorizes access to the information systems that receive, process, store or transmit PII based on valid access authorization, need-to-know permission or under the authority to re- disclose PII. j. Review accounts for compliance with account management requirements according to organization-based frequency; and k. Establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.
<p>Supplemental Guidance (from NIST 800-53)</p>	<p>Information system account types include, for example, individual, shared, group, system, guest/anonymous, emergency, developer/manufacturer/vendor, temporary, and service. Some of the account management requirements listed above can be implemented by organizational information systems. The identification of authorized users of the information system and the specification of access privileges reflects the requirements in other security controls in the security plan. Users requiring administrative privileges on information system accounts receive additional scrutiny by appropriate organizational personnel (e.g., system owner, mission/business owner, or chief information security officer) responsible for approving such accounts and privileged access. Organizations may choose to define access privileges or other attributes by account, by type of account, or a combination of both. Other attributes required for authorizing access include, for example, restrictions on time-of-day, day-of-week, and point-of-origin. In defining other account attributes, organizations consider system-related requirements (e.g., scheduled maintenance, system upgrades) and mission/business requirements, (e.g., time zone differences, customer requirements, remote access to support travel requirements). Failure to consider these factors could affect information system availability. Temporary and emergency accounts are accounts intended for short-term use. Organizations establish temporary accounts as a part of normal account activation procedures when there is a need for short-term accounts without the demand for immediacy in account activation. Organizations establish emergency accounts in response to crisis situations and with the need for rapid account activation. Therefore, emergency account activation may bypass normal account authorization processes. Emergency and temporary accounts are not to be confused with infrequently used accounts (e.g., local logon accounts used for special tasks defined by organizations or when network resources are unavailable). Such accounts remain available and are not subject to automatic disabling or removal dates. Conditions for disabling or deactivating accounts include, for example: (i) when shared/group, emergency, or temporary accounts are no longer required; or (ii) when individuals are transferred or terminated. Some types of information system accounts may require specialized training. Related controls: AC- 3, AC-4, AC-5, AC-6, AC-10, AC-17, AC-19, AC-20, AU-9, IA-2, IA-4, IA-5, IA-8, CM-5, CM-6, CM-11, MA-3, MA-4, MA-5, PL-4, SC-13.</p>
<p>Control Number</p>	<p>AC-3</p>
<p>Title</p>	<p>Account Management</p>
<p>DHCS & CDSS Requirement</p>	<p>The organization must:</p>

	<ul style="list-style-type: none"> a. Identify and select the accounts with access to PII to support organizational missions/business functions. b. Assign account managers for information system accounts; c. Establish conditions for group and role membership; d. Specify authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account; e. Require approvals by designated access authority for requests to create information system accounts; f. Create, enable, modify, disable, and remove information system accounts in accordance with organization account management procedures; g. Monitors the use of information system accounts; h. Notifies account managers when accounts are no longer required, when users are terminated or transferred; and when individual information system usage or need-to-know changes. i. Authorizes access to the information systems that receive, process, store or transmit PII based on valid access authorization, need-to-know permission or under the authority to re- disclose PII. j. Review accounts for compliance with account management requirements according to organization-based frequency; and k. Establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.
<p>Supplemental Guidance (from NIST 800-53)</p>	<p>Information system account types include, for example, individual, shared, group, system, guest/anonymous, emergency, developer/manufacturer/vendor, temporary, and service. Some of the account management requirements listed above can be implemented by organizational information systems. The identification of authorized users of the information system and the specification of access privileges reflects the requirements in other security controls in the security plan. Users requiring administrative privileges on information system accounts receive additional scrutiny by appropriate organizational personnel (e.g., system owner, mission/business owner, or chief information security officer) responsible for approving such accounts and privileged access. Organizations may choose to define access privileges or other attributes by account, by type of account, or a combination of both. Other attributes required for authorizing access include, for example, restrictions on time-of-day, day-of-week, and point-of-origin. In defining other account attributes, organizations consider system-related requirements (e.g., scheduled maintenance, system upgrades) and mission/business requirements, (e.g., time zone differences, customer requirements, remote access to support travel requirements). Failure to consider these factors could affect information system availability. Temporary and emergency accounts are accounts intended for short-term use. Organizations establish temporary accounts as a part of normal account activation procedures when there is a need for short-term accounts without the demand for immediacy in account activation. Organizations establish emergency accounts in response to crisis situations and with the need for rapid account activation. Therefore, emergency account activation may bypass normal account authorization processes. Emergency and temporary accounts are not to be confused with infrequently used accounts (e.g., local logon accounts used for special tasks defined by organizations or when network resources are unavailable). Such accounts</p>

	remain available and are not subject to automatic disabling or removal dates. Conditions for disabling or deactivating accounts include, for example: (i) when shared/group, emergency, or temporary accounts are no longer required; or (ii) when individuals are transferred or terminated. Some types of information system accounts may require specialized training. Related controls: AC- 3, AC-4, AC-5, AC-6, AC-10, AC-17, AC-19, AC-20, AU-9, IA-2, IA-4, IA-5, IA-8, CM-5, CM-6, CM-11, MA-3, MA-4, MA-5, PL-4, SC-13.
Control Number	AC-3(7)
Title	Access Enforcement Role-Based Access Control
DHCS & CDSS Requirement	The organization information system must: enforce a role-based access control policy over defined subjects and objects and controls access based upon the need to utilize PII.
Supplemental Guidance (from NIST 800-53)	Role-based access control (RBAC) is an access control policy that restricts information system access to authorized users. Organizations can create specific roles based on job functions and the authorizations (i.e., privileges) to perform needed operations on organizational information systems associated with the organization-defined roles. When users are assigned to the organizational roles, they inherit the authorizations or privileges defined for those roles. RBAC simplifies privilege administration for organizations because privileges are not assigned directly to every user (which can be a significant number of individuals for mid- to large-size organizations) but are instead acquired through role assignments. RBAC can be implemented either as a mandatory or discretionary form of access control. For organizations implementing RBAC with mandatory access controls, the requirements in AC-3 (3) define the scope of the subjects and objects covered by the policy.
Control Number	AC-3(8)
Title	Access Enforcement Revocation of Access Authorization
DHCS & CDSS Requirement	The organization must: Enforce a role-based access control over users and information resources that have access to PII, and control access based upon organization defined roles and users authorized to assume such roles.
Supplemental Guidance (from NIST 800-53)	Revocation of access rules may differ based on the types of access revoked. For example, if a subject (i.e., user or process) is removed from a group, access may not be revoked until the next time the object (e.g., file) is opened or until the next time the subject attempts a new access to the object. Revocation based on changes to security labels may take effect immediately. Organizations can provide alternative approaches on how to make revocations immediate if information systems cannot provide such capability and immediate revocation is necessary.
Control Number	AC-4
Title	Information Flow Enforcement
DHCS & CDSS Requirement	The organization information system must: enforce approved authorizations for controlling the flow of information within the system and between interconnected systems

	<p>based on the need for interconnected systems to share PII to conduct business.</p>
<p>Supplemental Guidance (from NIST 800-53)</p>	<p>Information flow control regulates where information is allowed to travel within an information system and between information systems (as opposed to who is allowed to access the information) and without explicit regard to subsequent accesses to that information. Flow control restrictions include, for example, keeping export-controlled information from being transmitted in the clear to the Internet, blocking outside traffic that claims to be from within the organization, restricting web requests to the Internet that are not from the internal web proxy server, and limiting information transfers between organizations based on data structures and content.</p> <p>Transferring information between information systems representing different security domains with different security policies introduces risk that such transfers violate one or more domain security policies. In such situations, information owners/stewards provide guidance at designated policy enforcement points between interconnected systems. Organizations consider mandating specific architectural solutions when required to enforce specific security policies. Enforcement includes, for example: (i) prohibiting information transfers between interconnected systems (i.e., allowing access only); (ii) employing hardware mechanisms to enforce one-way information flows; and (iii) implementing trustworthy regrading mechanisms to reassign security attributes and security labels.</p> <p>Organizations commonly employ information flow control policies and enforcement mechanisms to control the flow of information between designated sources and destinations (e.g., networks, individuals, and devices) within information systems and between interconnected systems. Flow control is based on the characteristics of the information and/or the information path.</p> <p>Enforcement occurs, for example, in boundary protection devices (e.g., gateways, routers, guards, encrypted tunnels, firewalls) that employ rule sets or establish configuration settings that restrict information system services, provide a packet-filtering capability based on header information, or message-filtering capability based on message content (e.g., implementing key word searches or using document characteristics). Organizations also consider the trustworthiness of filtering/inspection mechanisms (i.e., hardware, firmware, and software components) that are critical to information flow enforcement.</p> <p>Control enhancements 3 through 22 primarily address cross-domain solution needs which focus on more advanced filtering techniques, in-depth analysis, and stronger flow enforcement mechanisms implemented in cross-domain products, for example, high-assurance guards. Such capabilities are generally not available in commercial off-the-shelf information technology products. Related controls: AC-3, AC-17, AC-19, AC-21, CM-6, CM-7, SA-8, SC-2, SC-5, SC-7, SC-18</p>
<p>Control Number</p>	<p>AC-5</p>
<p>Title</p>	<p>Separation of Duties</p>
<p>DHCS & CDSS Requirement</p>	<p>The organization must:</p> <ul style="list-style-type: none"> a. Separate organization-defined duties of individuals; b. Document separation of duties of individuals; and c. Defines information system access authorizations to support separation of duties. <p><i>DHCS and CDSS also require that the state organization prohibit any functional</i></p>

	<p><i>component(s) or official(s) from issuing credentials or access authority to themselves or other individuals within their job- function or category of access.</i></p> <p><i>Federal requirements and DHCS and CDSS policy exclude any employee who uses PII to process programmatic workloads to make benefit or entitlement determinations from participation in management or quality assurance functions.</i></p>
Supplemental Guidance (from NIST 800-53)	<p>Separation of duties addresses the potential for abuse of authorized privileges and helps to reduce the risk of malevolent activity without collusion. Separation of duties includes, for example:</p> <p>(i) dividing mission functions and information system support functions among different individuals and/or roles; (ii) conducting information system support functions with different individuals (e.g., system management, programming, configuration management, quality assurance and testing, and network security); and (iii) ensuring security personnel administering access control functions do not also administer audit functions. Related controls: AC-3, AC-6, PE-3, PE-4, PS-2.</p>
Control Number	AC-6
Title	Least Privilege
DHCS & CDSS Requirement	<p>The organization must:</p> <p>Employ the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.</p>
Supplemental Guidance (from NIST 800-53)	<p>Organizations employ least privilege for specific duties and information systems. The principle of least privilege is also applied to information system processes, ensuring that the processes operate at privilege levels no higher than necessary to accomplish required organizational missions/business functions. Organizations consider the creation of additional processes, roles, and information system accounts as necessary, to achieve least privilege. Organizations also apply least privilege to the development, implementation, and operation of organizational information systems. Related controls: AC-2, AC-3, AC-5, CM-6, CM-7, PL-2.</p>
Control Number	AC-6(1)
Title	Least Privilege Authorize Access to Security Functions
DHCS & CDSS Requirement	<p>The organization must explicitly authorize access to organization-defined security functions (deployed in hardware, software, and firmware) and security-relevant information.</p>
Supplemental Guidance (from NIST 800-53)	<p>Security functions include, for example, establishing system accounts, configuring access authorizations (i.e., permissions, privileges), setting events to be audited, and setting intrusion detection parameters. Security-relevant information includes, for example, filtering rules for routers/firewalls, cryptographic key management information, configuration parameters for security services, and access control lists. Explicitly authorized personnel include, for example, security administrators, system and network administrators, system security officers, system maintenance personnel, system programmers, and other privileged users.</p>
Control	AC-6(7)

Number	
Title	Least Privilege Review Of User Privileges
DHCS & CDSS Requirement	<p>The organization must:</p> <ul style="list-style-type: none"> a. Review the privileges assigned to organization-defined roles or classes of users to validate the need for such privileges; and b. Reassign or removes privileges, if necessary, to correctly reflect organizational mission/business needs.
Supplemental Guidance (from NIST 800-53)	<p>The need for certain assigned user privileges may change over time reflecting changes in organizational missions/business function, environments of operation, technologies, or threat. Periodic review of assigned user privileges is necessary to determine if the rationale for assigning such privileges remains valid. If the need cannot be revalidated, organizations take appropriate corrective actions. Related control: CA-7.</p>
Control Number	AC-7
Title	Unsuccessful Logon Attempts
DHCS & CDSS Requirement	<p>The organization must:</p> <ul style="list-style-type: none"> a. Enforce a limit of no fewer than three (3) and no greater than five (5) consecutive invalid logon attempts by a user during an organization-defined time period; and b. Automatically lock the account/node for: an organization-defined time period; or locks the account/node until released by an administrator; or delays next logon prompt according to organization-defined delay algorithm when the maximum number of unsuccessful attempts is exceeded.
Supplemental Guidance (from NIST 800-53)	<p>This control applies regardless of whether the logon occurs via a local or network connection. Due to the potential for denial of service, automatic lockouts initiated by information systems are usually temporary and automatically release after a predetermined time period established by organizations. If a delay algorithm is selected, organizations may choose to employ different algorithms for different information system components based on the capabilities of those components. Responses to unsuccessful logon attempts may be implemented at both the operating system and the application levels. Related controls: AC-2, AC-9, AC-14, IA-5.</p>
Control Number	AC-8
Title	System Use Notification
DHCS & CDSS Requirement	<p>The organization must:</p> <ul style="list-style-type: none"> a. Displays to users system use notification message or banner before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance and states that: <ul style="list-style-type: none"> 1. Users are accessing a U.S. Government information system; 2. Information system usage may be monitored, recorded, and subject to audit; 3. Unauthorized use of the information system is prohibited and subject to criminal and civil penalties; and 4. Use of the information system indicates consent to monitoring and recording;

	<ul style="list-style-type: none"> b. Retains the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the information system; and c. For publicly accessible systems: <ul style="list-style-type: none"> 1. Displays system use information organization-defined conditions, before granting further access; 2. Displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and 3. Includes a description of the authorized uses of the system. <p>At a minimum, this can be done at initial logon and is not required for every logon.</p>
Supplemental Guidance (from NIST 800-53)	System use notifications can be implemented using messages or warning banners displayed before individuals log in to information systems. System use notifications are used only for access via logon interfaces with human users and are not required when such human interfaces do not exist. Organizations consider system use notification messages/banners displayed in multiple languages based on specific organizational needs and the demographics of information system users. Organizations also consult with the Office of the General Counsel for legal review and approval of warning banner content.
Control Number	AC-11
Title	Session Lock
DHCS & CDSS Requirement	<p>The organization's information system:</p> <ul style="list-style-type: none"> a. Prevents further access to the system by initiating a session lock after 15 minutes or upon receiving a request from a user; and b. Retains the session lock until the user reestablishes access using established identification and authentication procedures.
Supplemental Guidance (from NIST 800-53)	Session locks are temporary actions taken when users stop work and move away from the immediate vicinity of information systems but do not want to log out because of the temporary nature of their absences. Session locks are implemented where session activities can be determined. This is typically at the operating system level, but can also be at the application level. Session locks are not an acceptable substitute for logging out of information systems, for example, if organizations require users to log out at the end of workdays. Related control: AC-7.
Control Number	AC-17
Title	Remote Access
DHCS & CDSS Requirement	<p>The organization must:</p> <ul style="list-style-type: none"> a. Establish and document usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; and b. Authorize remote access to the information system prior to allowing such connections.
Supplemental Guidance (from NIST 800-53)	Remote access is access to organizational information systems by users (or processes acting on behalf of users) communicating through external networks (e.g., the Internet).

NIST 800-53)	<p>Remote access methods include, for example, dial-up, broadband, and wireless. Organizations often employ encrypted virtual private networks (VPNs) to enhance confidentiality and integrity over remote connections. The use of encrypted VPNs does not make the access non-remote; however, the use of VPNs, when adequately provisioned with appropriate security controls (e.g., employing appropriate encryption techniques for confidentiality and integrity protection) may provide sufficient assurance to the organization that it can effectively treat such connections as internal networks. Still, VPN connections traverse external networks, and the encrypted VPN does not enhance the availability of remote connections. Also, VPNs with encrypted tunnels can affect the organizational capability to adequately monitor network communications traffic for malicious code. Remote access controls apply to information systems other than public web servers or systems designed for public access. This control addresses authorization prior to allowing remote access without specifying the formats for such authorization. While organizations may use interconnection security agreements to authorize remote access connections, such agreements are not required by this control. Enforcing access restrictions for remote connections is addressed in AC-3. Related controls: AC-2, AC-3, AC-18, AC-19, AC-20, CA-3, CA-7, CM-8, IA-2, IA-3, IA-8, MA-4, PE-17, PL-4, SC-10, SI-4.</p>
---------------------	---

2. Accountability, Audit, and Risk Management (AR)

Control Number	AR-3
Title	Privacy Requirements for Contractors and Service Providers
DHCS & CDSS Requirement	<p>The organization must:</p> <ul style="list-style-type: none"> a. Establish privacy roles, responsibilities, and access requirements for contractors and service providers; and b. Includes privacy requirements in contracts and other acquisition-related documents.
Supplemental Guidance (from NIST 800-53)	<p>Contractors and service providers include, but are not limited to, information providers, information processors, and other organizations providing information system development, information technology services, and other outsourced applications. Organizations consult with legal counsel, the Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO), and contracting officers about applicable laws, directives, policies, or regulations that may impact implementation of this control. Related control: AR-1, AR-5, SA-4.</p>

3. Audit and Accountability (AU)

Control Number	AU-1
Title	Audit and Accountability Policy and Procedures
DHCS & CDSS Requirement	<p>The organization must:</p> <ul style="list-style-type: none"> a. Develop, document, and disseminate to individuals and organizations that store, process, or transmit PII: <ul style="list-style-type: none"> 1. An audit and accountability policy that addresses purpose, scope, roles,

	<p>responsibilities, management commitment, coordination among organizational entities, and compliance; and</p> <ol style="list-style-type: none"> 2. Procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls; and <p>b. Review and update the current:</p> <ol style="list-style-type: none"> 1. Audit and accountability policy at least triennially; and 2. Audit and accountability procedures at least triennially.
<p>Supplemental Guidance (from NIST 800-53)</p>	<p>This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the AU family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.</p>
<p>Control Number</p>	<p>AU-2</p>
<p>Title</p>	<p>Audit Events</p>
<p>DHCS & CDSS Requirement</p>	<p>The organization must:</p> <ol style="list-style-type: none"> a. Audit the following events: <ol style="list-style-type: none"> 1. Viewing PII stored within the organization’s system; 2. Viewing of screens that contain PII; 3. All system and data interactions concerning PII. b. Coordinate the security audit function with other organizational entities requiring audit-related information to enhance mutual support and to help guide the selection of auditable events; c. Determines that the following events are to be audited within the information system: <ol style="list-style-type: none"> 1. Viewing PII stored within the organization’s system; 2. Viewing of screens that contain PII; 3. All system and data interactions concerning PII.
<p>Supplemental Guidance (from NIST 800-53)</p>	<p>An event is any observable occurrence in an organizational information system. Organizations identify audit events as those events which are significant and relevant to the security of information systems and the environments in which those systems operate in order to meet specific and ongoing audit needs. Audit events can include, for example, password changes, failed logons, or failed accesses related to information systems, administrative privilege usage, PIV credential usage, or third-party credential usage. In determining the set of auditable events, organizations consider the auditing appropriate for each of the security controls to be implemented. To balance auditing requirements with other information system needs, this control also requires identifying that subset of auditable events that are audited at a given point in time. For example, organizations may determine that information systems must have the capability to log every file access both</p>

	<p>successful and unsuccessful, but not activate that capability except for specific circumstances due to the potential burden on system performance. Auditing requirements, including the need for auditable events, may be referenced in other security controls and control enhancements. Organizations also include auditable events that are required by applicable federal laws, Executive Orders, directives, policies, regulations, and standards. Audit records can be generated at various levels of abstraction, including at the packet level as information traverses the network. Selecting the appropriate level of abstraction is a critical aspect of an audit capability and can facilitate the identification of root causes to problems.</p> <p>Organizations consider in the definition of auditable events, the auditing necessary to cover related events such as the steps in distributed, transaction-based processes (e.g., processes that are distributed across multiple organizations) and actions that occur in service-oriented architectures. Related controls: AC-6, AC-17, AU-3, AU-12, MA-4, MP-2, MP-4, SI-4</p>
Control Number	AU-11
Title	Audit Record Retention
DHCS & CDSS Requirement	The organization must retain audit records for six (6) years to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.
Supplemental Guidance (from NIST 800-53)	Organizations retain audit records until it is determined that they are no longer needed for administrative, legal, audit, or other operational purposes. This includes, for example, retention and availability of audit records relative to Freedom of Information Act (FOIA) requests, subpoenas, and law enforcement actions. Organizations develop standard categories of audit records relative to such types of actions and standard response processes for each type of action. The National Archives and Records Administration (NARA) General Records Schedules provide federal policy on record retention. Related controls: AU-4, AU-5, AU-9, MP-6.
Control Number	AU-12
Title	Audit Generation
DHCS & CDSS Requirement	<p>The organization information system must:</p> <ol style="list-style-type: none"> a. Provide audit record generation capability for the auditable events defined in AU-2 a. at the audit reporting mechanism; b. Allow security personnel to select which auditable events are to be audited by specific components of the information system; and c. Generates audit records for the events defined in AU-2 d. with the content defined in AU-3
Supplemental Guidance (from NIST 800-53)	Audit records can be generated from many different information system components. The list of audited events is the set of events for which audits are to be generated. These events are typically a subset of all events for which the information system is capable of generating audit records. Related controls: AC-3, AU-2, AU-3, AU-6, AU-7.

4. Awareness and Training (AT)

Control Number	AT-1
Title	Security Awareness and Training Policy and Procedures
DHCS & CDSS Requirement	<p>The organization must:</p> <ul style="list-style-type: none"> a. Develop, document, and disseminate to personnel and organizations with access to PII: <ul style="list-style-type: none"> 1. A security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls; and b. Reviews and updates the current: <ul style="list-style-type: none"> 1. Security awareness and training policy and; 2. Security awareness and training procedures. <p>The training and awareness programs must include: The sensitivity of PII, The rules of behavior concerning use and security in systems and/or applications processing PII, The Privacy Act and other Federal and state laws, including but not limited to Section 14100.2 of the Welfare and Institutions Code and Section 431.302 et. Seq. of Title 42 Code of Federal Regulations, governing collection, maintenance, use, and dissemination of information about individuals, The possible criminal and civil sanctions and penalties for misuse of PII, The responsibilities of employees, contractors, and agent’s pertaining to the proper use and protection of PII, The restrictions on viewing and/or copying PII, The proper disposal of PII, The security breach and data loss incident reporting procedures, The basic understanding of procedures to protect the network from viruses, worms, Trojan horses, and other malicious code, Social engineering (phishing, vishing and pharming) and network fraud prevention.</p>
Supplemental Guidance (from NIST 800-53)	<p>This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the AT family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.</p>
Control	AT-2

Number	
Title	Security Awareness Training
DHCS & CDSS Requirement	The organization must provide basic security awareness training to information system users (including managers, senior executives, and contractors): <ul style="list-style-type: none"> a. As part of initial training for new users; b. When required by information system changes; and c. Annually thereafter.
Supplemental Guidance (from NIST 800-53)	Organizations determine the appropriate content of security awareness training and security awareness techniques based on the specific organizational requirements and the information systems to which personnel have authorized access. The content includes a basic understanding of the need for information security and user actions to maintain security and to respond to suspected security incidents. The content also addresses awareness of the need for operations security. Security awareness techniques can include, for example, displaying posters, offering supplies inscribed with security reminders, generating email advisories/notices from senior organizational officials, displaying logon screen messages, and conducting information security awareness events. Related controls: AT-3, AT-4, PL-4.
Control Number	AT-3
Title	Role-Based Security Training
DHCS & CDSS Requirement	The organization must provide role-based security training to personnel with assigned security roles and responsibilities: <ul style="list-style-type: none"> a. Before authorizing access to the information system or performing assigned duties; b. When required by information system changes; and c. With organization-defined frequency thereafter.
Supplemental Guidance (from NIST 800-53)	Organizations determine the appropriate content of security training based on the assigned roles and responsibilities of individuals and the specific security requirements of organizations and the information systems to which personnel have authorized access. In addition, organizations provide enterprise architects, information system developers, software developers, acquisition/procurement officials, information system managers, system/network administrators, personnel conducting configuration management and auditing activities, personnel performing independent verification and validation activities, security control assessors, and other personnel having access to system-level software, adequate security-related technical training specifically tailored for their assigned duties. Comprehensive role-based training addresses management, operational, and technical roles and responsibilities covering physical, personnel, and technical safeguards and countermeasures. Such training can include for example, policies, procedures, tools, and artifacts for the organizational security roles defined. Organizations also provide the training necessary for individuals to carry out their responsibilities related to operations and supply chain security within the context of organizational information security programs. Role- based security training also applies to contractors providing services to federal agencies. Related controls: AT-2, AT-4, PL-4, PS-7, SA-3, SA-12, SA-16.
Control Number	AT-4
Title	Security Training Records

<p>DHCS & CDSS Requirement</p>	<p>The organization must:</p> <ul style="list-style-type: none"> a. Document and monitor individual information system security training activities including basic security awareness training and specific information system security training; and b. Retain individual training records for 5 years. <p>SSA also requires the organization to certify that each employee, contractor, and agent who views SSA data certify that they understand the potential criminal, civil, and administrative sanctions or penalties for unlawful assess and/or disclosure.</p>
<p>Supplemental Guidance (from NIST 800-53)</p>	<p>Documentation for specialized training may be maintained by individual supervisors at the option of the organization. Related controls: AT-2, AT-3, PM-14.</p>

5. Contingency Planning (CP)

<p>Control Number</p>	<p>CP-2</p>
<p>Title</p>	<p>Contingency Plan</p>
<p>DHCS & CDSS Requirement</p>	<p>The organization must:</p> <ul style="list-style-type: none"> a. Develop a contingency plan for the information system that: <ul style="list-style-type: none"> 1. Identifies essential missions and business functions and associated contingency requirements; 2. Provides recovery objectives, restoration priorities, and metrics; 3. Addresses contingency roles, responsibilities, assigned individuals with contact information; 4. Addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure; 5. Addresses eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented; and 6. Is reviewed and approved by a senior manager; b. Distribute copies of the contingency plan to personnel and organizations supporting the contingency plan actions; c. Coordinate contingency planning activities with incident handling activities; d. Review the contingency plan for the information system at least annually; e. Update the contingency plan to address changes to the organization, information system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing; f. Communicate contingency plan changes to personnel and organizations supporting the contingency plan actions; g. Incorporate lessons learned from contingency plan testing, training, or actual contingency activities into contingency testing and training; and h. Protect the contingency plan from unauthorized disclosure and modification.
<p>Supplemental Guidance (from</p>	<p>Contingency planning for information systems is part of an overall organizational program for achieving continuity of operations for mission/business functions. Contingency planning</p>

NIST 800-53)	<p>addresses both information system restoration and implementation of alternative mission/business processes when systems are compromised. The effectiveness of contingency planning is maximized by considering such planning throughout the phases of the system development life cycle. Performing contingency planning on hardware, software, and firmware development can be an effective means of achieving information system resiliency. Contingency plans reflect the degree of restoration required for organizational information systems since not all systems may need to fully recover to achieve the level of continuity of operations desired.</p> <p>Information system recovery objectives reflect applicable laws, Executive Orders, directives, policies, standards, regulations, and guidelines. In addition to information system availability, contingency plans also address other security-related events resulting in a reduction in mission and/or business effectiveness, such as malicious attacks compromising the confidentiality or integrity of information systems. Actions addressed in contingency plans include, for example, orderly/graceful degradation, information system shutdown, fallback to a manual mode, alternate information flows, and operating in modes reserved for when systems are under attack. By closely coordinating contingency planning with incident handling activities, organizations can ensure that the necessary contingency planning activities are in place and activated in the event of a security incident. Related controls: AC-14, CP-6, CP-7, CP-8, CP-9, CP-10, IR-4, IR-8, MP-2, MP-4, MP-5, PM-8, PM-11.</p>
---------------------	--

6. Data Minimization and Retention (DM)

Control Number	DM-2
Title	Data Retention and Disposal
DHCS & CDSS Requirement	<p>The organization must:</p> <ol style="list-style-type: none"> a. Retain each collection of PII no longer than required for the organization’s business process or evidentiary purposes; b. Dispose of, destroys, erases, and/or anonymizes the PII, regardless of the method of storage, in accordance with a NARA-approved record retention schedule and in a manner that prevents loss, theft, misuse, or unauthorized access; and c. Use organization-defined techniques or methods to ensure secure deletion or destruction of PII (including originals, copies, and archived records).
Supplemental Guidance (from NIST 800-53)	<p>NARA provides retention schedules that govern the disposition of federal records. Program officials coordinate with records officers and with NARA to identify appropriate retention periods and disposal methods. NARA may require organizations to retain PII longer than is operationally needed. In those situations, organizations describe such requirements in the notice. Methods of storage include, for example, electronic, optical media, or paper.</p> <p>Examples of ways organizations may reduce holdings include reducing the types of PII held (e.g., delete Social Security numbers if their use is no longer needed) or shortening the retention period for PII that is maintained if it is no longer necessary to keep PII for long periods of time (this effort is undertaken in consultation with an organization’s records officer to receive NARA approval). In both examples, organizations provide notice (e.g., an updated System of Records Notice) to inform the public of any changes in holdings of PII. Certain read-only archiving techniques, such as DVDs, CDs, microfilm, or microfiche, may</p>

	not permit the removal of individual records without the destruction of the entire database contained on such media. Related controls: AR-4, AU-11, DM-1, MP-1, MP-2, MP-3, MP-4, MP-5, MP-6, MP-7, MP-8, SI-12, TR-1.
--	--

7. Identification and Authentication (IA)

Control Number	IA-2
Title	Identification and Authentication (Organizational Users)
DHCS & CDSS Requirement	The organization's information system must uniquely identify and authenticate organizational users (or processes acting on behalf of organizational users).
Supplemental Guidance (from NIST 800-53)	<p>Organizational users include employees or individuals that organizations deem to have equivalent status of employees (e.g., contractors, guest researchers). This control applies to all accesses other than: (i) accesses that are explicitly identified and documented in AC-14; and (ii) accesses that occur through authorized use of group authenticators without individual authentication.</p> <p>Organizations may require unique identification of individuals in group accounts (e.g., shared privilege accounts) or for detailed accountability of individual activity. Organizations employ passwords, tokens, or biometrics to authenticate user identities, or in the case multifactor authentication, or some combination thereof. Access to organizational information systems is defined as either local access or network access. Local access is any access to organizational information systems by users (or processes acting on behalf of users) where such access is obtained by direct connections without the use of networks. Network access is access to organizational information systems by users (or processes acting on behalf of users) where such access is obtained through network connections (i.e., nonlocal accesses). Remote access is a type of network access that involves communication through external networks (e.g., the Internet). Internal networks include local area networks and wide area networks. In addition, the use of encrypted virtual private networks (VPNs) for network connections between organization- controlled endpoints and non-organization controlled endpoints may be treated as internal networks from the perspective of protecting the confidentiality and integrity of information traversing the network.</p> <p>Organizations can satisfy the identification and authentication requirements in this control by complying with the requirements in Homeland Security Presidential Directive 12 consistent with the specific organizational implementation plans. Multifactor authentication requires the use of two or more different factors to achieve authentication. The factors are defined as: (i) something you know (e.g., password, personal identification number [PIN]); (ii) something you have (e.g., cryptographic identification device, token); or (iii) something you are (e.g., biometric). Multifactor solutions that require devices separate from information systems gaining access include, for example, hardware tokens providing time-based or challenge-response authenticators and smart cards such as the U.S. Government Personal Identity Verification card and the DoD common access card. In addition to identifying and authenticating users at the information system level (i.e., at logon), organizations also employ identification and authentication mechanisms at the application level, when necessary, to provide increased information security. Identification and authentication requirements for other than organizational users are described in IA-8. Related controls: AC-2, AC-3, AC-14, AC-17, AC-18, IA-4, IA-5, IA-8.</p>
Control	IA-5

Number	
Title	Authenticator Management
DHCS & CDSS Requirement	<p>The organization must manage information system authenticators by:</p> <ol style="list-style-type: none"> a. Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, or device receiving the authenticator; b. Establishing initial authenticator content for authenticators defined by the organization; c. Ensuring that authenticators have sufficient strength of mechanism for their intended use; d. Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators; e. Changing default content of authenticators prior to information system installation; f. Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators; g. Changing/refreshing authenticators within organization-defined time period; h. Protecting authenticator content from unauthorized disclosure and modification; i. Requiring individuals to take, and having devices implement, specific security safeguards to protect authenticators; and j. Changing authenticators for group/role accounts when membership to those accounts changes.
Supplemental Guidance (from NIST 800-53)	<p>Individual authenticators include, for example, passwords, tokens, biometrics, PKI certificates, and key cards. Initial authenticator content is the actual content (e.g., the initial password) as opposed to requirements about authenticator content (e.g., minimum password length). In many cases, developers ship information system components with factory default authentication credentials to allow for initial installation and configuration. Default authentication credentials are often well known, easily discoverable, and present a significant security risk. The requirement to protect individual authenticators may be implemented via control PL-4 or PS-6 for authenticators in the possession of individuals and by controls AC-3, AC-6, and SC-28 for authenticators stored within organizational information systems (e.g., passwords stored in hashed or encrypted formats, files containing encrypted or hashed passwords accessible with administrator privileges).</p> <p>Information systems support individual authenticator management by organization-defined settings and restrictions for various authenticator characteristics including, for example, minimum password length, password composition, validation time window for time synchronous one-time tokens, and number of allowed rejections during the verification stage of biometric authentication. Specific actions that can be taken to safeguard authenticators include, for example, maintaining possession of individual authenticators, not loaning or sharing individual authenticators with others, and reporting lost, stolen, or compromised authenticators immediately. Authenticator management includes issuing and revoking, when no longer needed, authenticators for temporary access such as that required for remote maintenance. Device authenticators include, for example, certificates and passwords. Related controls: AC-2, AC-3, AC-6, CM-6, IA-2, IA-4, IA-8, PL-4, PS- 5, PS-6, SC-12, SC-13, SC-17, SC-28.</p>
Control	IA-5(1)

Number	
Title	Authenticator Management Password-Based Authentication
DHCS & CDSS Requirement	<p>The information system, for password-based authentication, must:</p> <ul style="list-style-type: none"> a. Enforces minimum password complexity of requirements for: <ul style="list-style-type: none"> * case sensitivity (upper and lower case letters), * number of characters (equal to or greater than fifteen characters), * mix of upper-case letters, lower-case letters, numbers, and special characters (at least one of each type); c. Stores and transmits only cryptographically-protected passwords; d. Enforces password lifetime of at least 180 days; e. Prohibits prior 10 passwords for reuse; and f. Allows the use of a temporary password for system logons with an immediate change to a permanent password.
Supplemental Guidance (from NIST 800-53)	<p>This control enhancement applies to single-factor authentication of individuals using passwords as individual or group authenticators, and in a similar manner, when passwords are part of multifactor authenticators. This control enhancement does not apply when passwords are used to unlock hardware authenticators (e.g., Personal Identity Verification cards). The implementation of such password mechanisms may not meet all of the requirements in the enhancement.</p> <p>Cryptographically-protected passwords include, for example, encrypted versions of passwords and one-way cryptographic hashes of passwords. The number of changed characters refers to the number of changes required with respect to the total number of positions in the current password. Password lifetime restrictions do not apply to temporary passwords. To mitigate certain brute force attacks against passwords, organizations may also consider salting passwords.</p> <p>Related control: IA-6.</p>

8. Incident Response (IR)

Control Number	IR-1
Title	Incident Response Policy and Procedures
DHCS & CDSS Requirement	<p>The organization must:</p> <ul style="list-style-type: none"> a. Develops, documents, and disseminates to organization-defined personnel or roles: <ul style="list-style-type: none"> 1. An incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the incident response policy and associated incident response controls; and b. Reviews and updates the current: <ul style="list-style-type: none"> 1. Incident response policy with organization-defined frequency; and 2. Incident response procedures with organization-defined frequency. <p><i>DHCS, CDSS and NIST Guidelines encourage agencies to consider establishing incident response teams or identifying individuals specifically responsible for addressing PII, DHCS</i></p>

	and CDSS <i>data breaches</i> .
Supplemental Guidance (from NIST 800-53)	This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the IR family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.
Control Number	IR-2
Title	Incident Response Training
DHCS & CDSS Requirement	The organization must provide incident response training to information system users consistent with assigned roles and responsibilities: <ul style="list-style-type: none"> a. Within organization-defined time period of assuming an incident response role or responsibility; b. When required by information system changes; and c. With organization-defined frequency thereafter.
Supplemental Guidance (from NIST 800-53)	Incident response training provided by organizations is linked to the assigned roles and responsibilities of organizational personnel to ensure the appropriate content and level of detail is included in such training. For example, regular users may only need to know who to call or how to recognize an incident on the information system; system administrators may require additional training on how to handle/remediate incidents; and incident responders may receive more specific training on forensics, reporting, system recovery, and restoration. Incident response training includes user training in the identification and reporting of suspicious activities, both from external and internal sources. Related controls: AT-3, CP-3, IR-8.
Control Number	IR-4
Title	Incident Handling
DHCS & CDSS Requirement	The organization must: <ul style="list-style-type: none"> a. Implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery; b. Coordinates incident handling activities with contingency planning activities; and c. Incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing, and implements the resulting changes accordingly.
Supplemental Guidance (from NIST 800-53)	Organizations recognize that incident response capability is dependent on the capabilities of organizational information systems and the mission/business processes being supported by those systems. Therefore, organizations consider incident response as part of the definition, design, and development of mission/business processes and information systems. Incident-

	related information can be obtained from a variety of sources including, for example, audit monitoring, network monitoring, physical access monitoring, user/administrator reports, and reported supply chain events. Effective incident handling capability includes coordination among many organizational entities including, for example, mission/business owners, information system owners, authorizing officials, human resources offices, physical and personnel security offices, legal departments, operations personnel, procurement offices, and the risk executive (function). Related controls: AU-6, CM-6, CP-2, CP-4, IR-2, IR-3, IR-8, PE-6, SC-5, SC-7, SI-3, SI-4, SI-7.
Control Number	IR-8
Title	Incident Response Plan
DHCS & CDSS Requirement	<p>The organization must:</p> <ol style="list-style-type: none"> a. Develop an incident response plan that: <ol style="list-style-type: none"> 1. Provides the organization with a roadmap for implementing its incident response capability; 2. Describes the structure and organization of the incident response capability; 3. Provides a high-level approach for how the incident response capability fits into the overall organization; 4. Meets the unique requirements of the organization, which relate to mission, size, structure, and functions; 5. Defines reportable incidents; 6. Provides metrics for measuring the incident response capability within the organization; 7. Defines the resources and management support needed to effectively maintain and mature an incident response capability; and 8. Is reviewed and approved by organization-defined personnel or roles; b. Distribute copies of the incident response plan to organization-defined incident response personnel (identified by name and/or by role) and organizational elements; c. Review the incident response plan organization-defined frequency; d. Updates the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing; e. Communicate incident response plan changes to organization-defined incident response personnel (identified by name and/or by role) and organizational elements]; and f. Protect the incident response plan from unauthorized disclosure and modification.
Supplemental Guidance (from NIST 800-53)	It is important that organizations develop and implement a coordinated approach to incident response. Organizational missions, business functions, strategies, goals, and objectives for incident response help to determine the structure of incident response capabilities. As part of a comprehensive incident response capability, organizations consider the coordination and sharing of information with external organizations, including, for example, external service providers and organizations involved in the supply chain for organizational information systems. Related controls: MP-2, MP-4, MP-5.

9. Media Protection (MP)

Control Number	MP-2
Title	Media Access
DHCS & CDSS Requirement	The organization must: Restricts access to PII to Contractor Workers who require access to PII for purposes of administering the Medi-Cal program or as required for the administration of other public benefit programs.
Supplemental Guidance (from NIST 800-53)	Information system media includes both digital and non-digital media. Digital media includes, for example, diskettes, magnetic tapes, external/removable hard disk drives, flash drives, compact disks, and digital video disks. Non-digital media includes, for example, paper and microfilm. Restricting non-digital media access includes, for example, denying access to patient medical records in a community hospital unless the individuals seeking access to such records are authorized healthcare providers. Restricting access to digital media includes, for example, limiting access to design specifications stored on compact disks in the media library to the project leader and the individuals on the development team. Related controls: AC-3, IA-2, MP-4, PE-2, PE-3, PL-2.
Control Number	MP-6
Title	Media Sanitization
DHCS & CDSS Requirement	The organization must: <ul style="list-style-type: none"> a. Sanitize media containing PII prior to disposal, release out of organizational control, or release for reuse in accordance with applicable federal and organizational standards and policies; and b. Employs sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.
Supplemental Guidance (from NIST 800-53)	This control applies to all information system media, both digital and non-digital, subject to disposal or reuse, whether or not the media is considered removable. Examples include media found in scanners, copiers, printers, notebook computers, workstations, network components, and mobile devices. The sanitization process removes information from the media such that the information cannot be retrieved or reconstructed. Sanitization techniques, including clearing, purging, cryptographic erase, and destruction, prevent the disclosure of information to unauthorized individuals when such media is reused or released for disposal. Organizations determine the appropriate sanitization methods recognizing that destruction is sometimes necessary when other methods cannot be applied to media requiring sanitization. Organizations use discretion on the employment of approved sanitization techniques and procedures for media containing information deemed to be in the public domain or publicly releasable, or deemed to have no adverse impact on organizations or individuals if released for reuse or disposal. Sanitization of non-digital media includes, for example, removing a classified appendix from an otherwise unclassified document, or redacting selected sections or words from a document by obscuring the redacted sections/words in a manner equivalent in effectiveness to removing them from the document. NSA standards and policies control the sanitization process for media containing classified information. Related controls: MA-2, MA-4, RA-3, SC-4.

10. Personnel Security (PS)

Control Number	PS-3
Title	Personnel Screening
DHCS & CDSS Requirement	The organization must: <ul style="list-style-type: none"> a. Screen individuals (employees, contractors and agents) prior to authorizing access to the information system and PII.
Supplemental Guidance (from NIST 800-53)	Personnel screening and rescreening activities reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, guidance, and specific criteria established for the risk designations of assigned positions. Organizations may define different rescreening conditions and frequencies for personnel accessing information systems based on types of information processed, stored, or transmitted by the systems.
Control Number	PS-4
Title	Personnel Termination
DHCS & CDSS Requirement	The organization, upon termination of individual employment, must: <ul style="list-style-type: none"> a. Disable information system access; b. Terminate/revoke any authenticators/credentials associated with the individual; c. Conduct exit interviews, as needed; d. Retrieve all security-related organizational information system-related property; e. Retain access to organizational information and information systems formerly controlled by terminated individual; and f. Notified organization-defined personnel upon termination.
Supplemental Guidance (from NIST 800-53)	Information system-related property includes, for example, hardware authentication tokens, system administration technical manuals, keys, identification cards, and building passes. Exit interviews ensure that terminated individuals understand the security constraints imposed by being former employees and that proper accountability is achieved for information system-related property. Security topics of interest at exit interviews can include, for example, reminding terminated individuals of nondisclosure agreements and potential limitations on future employment. Exit interviews may not be possible for some terminated individuals, for example, in cases related to job abandonment, illnesses, and non-availability of supervisors. Exit interviews are important for individuals with security clearances. Timely execution of termination actions is essential for individuals terminated for cause. In certain situations, organizations consider disabling the information system accounts of individuals that are being terminated prior to the individuals being notified. Related controls: AC-2, IA-4, PE-2, PS-5, PS-6.
Control Number	PS-6
Title	Access Agreements
DHCS & CDSS Requirement	The organization must: <ul style="list-style-type: none"> a. Develop and document access agreements for organizational information systems; b. Reviews and updates the access agreements at organization-defined frequency; and c. Ensure that individuals requiring access to organizational information and information

	<p>systems:</p> <ol style="list-style-type: none"> 1. Sign appropriate access agreements prior to being granted access; and 2. Re-sign access agreements to maintain access to organizational information systems when access agreements have been updated or at an organization-defined frequency. <p>DHCS and CDSS requires that contracts for periodic disposal/destruction of case files or other print media contain a non-disclosure agreement signed by all personnel who will encounter products that contain PII.</p>
Supplemental Guidance (from NIST 800-53)	<p>Supplemental Guidance: Access agreements include, for example, nondisclosure agreements, acceptable use agreements, rules of behavior, and conflict-of-interest agreements. Signed access agreements include an acknowledgement that individuals have read, understand, and agree to abide by the constraints associated with organizational information systems to which access is authorized. Organizations can use electronic signatures to acknowledge access agreements unless specifically prohibited by organizational policy. Related control: PL-4, PS-2, PS-3, PS-4, PS-8.</p>
Control Number	PS-7
Title	Third-Party Personnel Security
DHCS & CDSS Requirement	<p>The organization must:</p> <ol style="list-style-type: none"> a. Establishes personnel security requirements including security roles and responsibilities for county agents, subcontractors, and vendors; b. Requires third-party providers to comply with personnel security policies and procedures established by the organization; c. Documents personnel security requirements; d. Requires third-party providers to notify organization-defined personnel or roles of any personnel transfers or terminations of third-party personnel who possess organizational credentials and/or badges, or who have information system privileges within organization-defined time period; and e. Monitors provider compliance. <p><i>The service level agreements with the contractors and agents must contain non-disclosure language as it pertains to PII. The statement shall include, at a minimum, a description of the following:</i></p> <ol style="list-style-type: none"> 1. <i>General Use of PII;</i> 2. <i>Security and Privacy Safeguards for PII;</i> 3. <i>Unacceptable Use of PII; and</i> 4. <i>Enforcement Policies.</i> <p><i>The county department/agency must retain the non-disclosure agreements for at least five (5) to seven (7) years for all contractors and agents who processes, views, or encounters PII as part of their duties</i></p>
Supplemental Guidance (from NIST 800-53)	<p>Third-party providers include, for example, service bureaus, contractors, and other organizations providing information system development, information technology services, outsourced applications, and network and security management. Organizations explicitly include personnel security requirements in acquisition-related documents. Third-party providers may have personnel working at organizational facilities with credentials, badges, or</p>

	information system privileges issued by organizations. Notifications of third-party personnel changes ensure appropriate termination of privileges and credentials. Organizations define the transfers and terminations deemed reportable by security-related characteristics that include, for example, functions, roles, and nature of credentials/privileges associated with individuals transferred or terminated. Related controls: PS-2, PS-3, PS-4, PS-5, PS-6, SA-9, SA-21.
Control Number	PS-8
Title	Personnel Sanctions
DHCS & CDSS Requirement	<p>The organization must:</p> <ul style="list-style-type: none"> a. Employ a formal sanctions process for individuals failing to comply with established information security policies and procedures; and b. Notify organization personnel within the organization-defined time period when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction. <p><i>If a member of the county's workforce, as defined at 45 CFR 160.103 and inclusive of an employee, contractor, or agent is subject to an adverse action by the organization (e.g., reduction in pay, disciplinary action, termination of employment, termination of contract for services), DHCS and CDSS recommends the organization remove his or her access to PII in advance of the adverse action to reduce the possibility that will the individual will perform unauthorized activities that involve PII, if applicable.</i></p>
Supplemental Guidance (from NIST 800-53)	Organizational sanctions processes reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Sanctions processes are described in access agreements and can be included as part of general personnel policies and procedures for organizations. Organizations consult with the Office of the General Counsel regarding matters of employee sanctions. Related controls: PL-4, PS-6.

11. Physical and Environmental Protection (PE)

Control Number	PE-3
Title	Physical Access Control
DHCS & CDSS Requirement	<p>The organization must:</p> <ul style="list-style-type: none"> a. Enforce physical access authorizations at entry and exit points to the facility where the information system resides by; <ul style="list-style-type: none"> 1. Verifying individual access authorizations before granting access to the facility; and 2. Controlling ingress/egress to the facility using physical access control systems/devices and/or guards; b. Maintain physical access audit logs for entry and exit points; c. Provide security safeguards to control access to areas within the facility officially designated as publicly accessible; d. Escort visitors and monitors visitor activity; e. Secure keys, combinations, and other physical access devices; f. Inventory physical access devices; and

	g. Changes combinations and keys at minimum when keys are lost, combinations are compromised, or individuals are transferred or terminated
Supplemental Guidance (from NIST 800-53)	<p>This control applies to organizational employees and visitors. Individuals (e.g., employees, contractors, and others) with permanent physical access authorization credentials are not considered visitors. Organizations determine the types of facility guards needed including, for example, professional physical security staff or other personnel such as administrative staff or information system users. Physical access devices include, for example, keys, locks, combinations, and card readers. Safeguards for publicly accessible areas within organizational facilities include, for example, cameras, monitoring by guards, and isolating selected information systems and/or system components in secured areas. Physical access control systems comply with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. The Federal Identity, Credential, and Access Management Program provides implementation guidance for identity, credential, and access management capabilities for physical access control systems. Organizations have flexibility in the types of audit logs employed. Audit logs can be procedural (e.g., a written log of individuals accessing the facility and when such access occurred), automated (e.g., capturing ID provided by a PIV card), or some combination thereof. Physical access points can include facility access points, interior access points to information systems and/or components requiring supplemental access controls, or both.</p> <p>Components of organizational information systems (e.g., workstations, terminals) may be located in areas designated as publicly accessible with organizations safeguarding access to such devices. Related controls: AU-2, AU-6, MP-2, MP-4, PE-2, PE-4, PE-5, PS-3, RA-3.</p>
Control Number	PE-6
Title	Monitoring Physical Access
DHCS & CDSS Requirement	<p>The organization must:</p> <ol style="list-style-type: none"> a. Monitors physical access to the facility where the information system resides to detect and respond to physical security incidents; b. Reviews physical access logs organization-defined frequency and upon occurrence of security incidents; and c. Coordinates results of reviews and investigations with the organizational incident response capability.
Supplemental Guidance (from NIST 800-53)	<p>Organizational incident response capabilities include investigations of and responses to detected physical security incidents. Security incidents include, for example, apparent security violations or suspicious physical access activities. Suspicious physical access activities include, for example:</p> <ol style="list-style-type: none"> (i) accesses outside of normal work hours; (ii) repeated accesses to areas not normally accessed; (iii) accesses for unusual lengths of time; and (iv) out-of-sequence accesses. <p>Related controls: CA-7, IR-4, IR-8.</p>

12. Planning (PL)

Control	PL-1
----------------	------

Number	
Title	Security Planning Policy and Procedures
DHCS & CDSS Requirement	<p>The organization must:</p> <ol style="list-style-type: none"> a. Develop, document, and disseminate to personnel and organizations with access to PII: <ol style="list-style-type: none"> 1. A security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the security planning policy and associated security planning controls; and b. Reviews and updates the current: <ol style="list-style-type: none"> 1. Security planning policy; and 2. Security planning procedures.
Supplemental Guidance (from NIST 800-53)	<p>This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the PL family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.</p>
Control Number	PL-2
Title	System Security Plan
DHCS & CDSS Requirement	<p>The organization must:</p> <ol style="list-style-type: none"> a. Develop a security plan for the information system that: <ol style="list-style-type: none"> 1. Is consistent with the organization’s enterprise architecture; 2. Explicitly defines the authorization boundary for the system; 3. Describes the operational context of the information system in terms of missions and business processes; 4. Provides the security categorization of the information system including supporting rationale; 5. Describes the operational environment for the information system and relationships with or connections to other information systems; 6. Provides an overview of the security requirements for the system; 7. Identifies any relevant overlays, if applicable; 8. Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring decisions; and 9. Is reviewed and approved by the authorizing official or designated representative prior to plan implementation; b. Distribute copies of the security plan and communicates subsequent changes to the plan to personnel and organizations with security responsibilities;

	<ul style="list-style-type: none"> c. Review the security plan for the information system; d. Update the plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments; and e. Protect the security plan from unauthorized disclosure and modification. <p><i>Organization's security plan should include detailed information specific to safeguarding Medi- Cal PII.</i></p>
<p>Supplemental Guidance (from NIST 800-53)</p>	<p>Security plans relate security requirements to a set of security controls and control enhancements. Security plans also describe, at a high level, how the security controls and control enhancements meet those security requirements, but do not provide detailed, technical descriptions of the specific design or implementation of the controls/enhancements. Security plans contain sufficient information (including the specification of parameter values for assignment and selection statements either explicitly or by reference) to enable a design and implementation that is unambiguously compliant with the intent of the plans and subsequent determinations of risk to organizational operations and assets, individuals, other organizations, and the Nation if the plan is implemented as intended. Organizations can also apply tailoring guidance to the security control baselines in Appendix D and CNSS Instruction 1253 to develop overlays for community-wide use or to address specialized requirements, technologies, or missions/environments of operation (e.g., DoD-tactical, Federal Public Key Infrastructure, or Federal Identity, Credential, and Access Management, space operations). Appendix I provides guidance on developing overlays.</p> <p>Security plans need not be single documents; the plans can be a collection of various documents including documents that already exist. Effective security plans make extensive use of references to policies, procedures, and additional documents (e.g., design and implementation specifications) where more detailed information can be obtained. This reduces the documentation requirements associated with security programs and maintains security-related information in other established management/operational areas related to enterprise architecture, system development life cycle, systems engineering, and acquisition. For example, security plans do not contain detailed contingency plan or incident response plan information but instead provide explicitly or by reference, sufficient information to define what needs to be accomplished by those plans. Related controls: AC-2, AC-6, AC-14, AC-17, AC-20, CA-2, CA-3, CA-7, CM-9, CP-2, IR-8, MA-4, MA-5, MP-2, MP-4, MP-5, PL-7, PM-1, PM-7, PM-8, PM-9, PM-11, SA-5, SA- 17.</p>

13. Risk Assessment (RA)

<p>Control Number</p>	<p>RA-1</p>
<p>Title</p>	<p>Risk Assessment Policy and Procedures</p>
<p>DHCS & CDSS Requirement</p>	<p>The organization must:</p> <ul style="list-style-type: none"> a. Develop, document, and disseminate to system owners using PII: <ul style="list-style-type: none"> 1. A risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls.

Supplemental Guidance (from NIST 800-53)	This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the RA family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.
Control Number	RA-3
Title	Risk Assessment
DHCS & CDSS Requirement	<p>The organization must:</p> <ul style="list-style-type: none"> a. Conduct an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits; b. Documents risk assessment results in a risk assessment report or organization defined risk report document. c. Review risk assessment results annually; and e. Update the risk assessment whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system.
Supplemental Guidance (from NIST 800-53)	<p>Clearly defined authorization boundaries are a prerequisite for effective risk assessments. Risk assessments take into account threats, vulnerabilities, likelihood, and impact to organizational operations and assets, individuals, other organizations, and the Nation based on the operation and use of information systems. Risk assessments also take into account risk from external parties (e.g., service providers, contractors operating information systems on behalf of the organization, individuals accessing organizational information systems, outsourcing entities). In accordance with OMB policy and related E-authentication initiatives, authentication of public users accessing federal information systems may also be required to protect nonpublic or privacy-related information. As such, organizational assessments of risk also address public access to federal information systems.</p> <p>Risk assessments (either formal or informal) can be conducted at all three tiers in the risk management hierarchy (i.e., organization level, mission/business process level, or information system level) and at any phase in the system development life cycle. Risk assessments can also be conducted at various steps in the Risk Management Framework, including categorization, security control selection, security control implementation, security control assessment, information system authorization, and security control monitoring. RA-3 is noteworthy in that the control must be partially implemented prior to the implementation of other controls in order to complete the first two steps in the Risk Management Framework. Risk assessments can play an important role in security control selection processes, particularly during the application of tailoring guidance, which includes security control supplementation. Related controls: RA-2, PM- 9.</p>
Control	RA-5

Number	
Title	Vulnerability Scanning
DHCS & CDSS Requirement	<p>The organization must:</p> <ol style="list-style-type: none"> a. Scan for vulnerabilities in the information system and hosted applications at a minimum of a monthly basis and when new vulnerabilities potentially affecting the system/applications are identified and reported; b. Employ vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for: <ol style="list-style-type: none"> 1. Enumerating platforms, software flaws, and improper configurations; <ol style="list-style-type: none"> a. Analyze vulnerability scan reports and results from security control assessments; b. Remediate legitimate vulnerabilities within organization defined time periods in accordance with an organizational assessment of risk; and c. Share information obtained from the vulnerability scanning process and security control assessments with all impacted system owners to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).
Supplemental Guidance (from NIST 800-53)	<p>Security categorization of information systems guides the frequency and comprehensiveness of vulnerability scans. Organizations determine the required vulnerability scanning for all information system components, ensuring that potential sources of vulnerabilities such as networked printers, scanners, and copiers are not overlooked. Vulnerability analyses for custom software applications may require additional approaches such as static analysis, dynamic analysis, binary analysis, or a hybrid of the three approaches. Organizations can employ these analysis approaches in a variety of tools (e.g., web-based application scanners, static analysis tools, binary analyzers) and in source code reviews. Vulnerability scanning includes, for example:</p> <p>(i) scanning for patch levels; (ii) scanning for functions, ports, protocols, and services that should not be accessible to users or devices; and (iii) scanning for improperly configured or incorrectly operating information flow control mechanisms. Organizations consider using tools that express vulnerabilities in the Common Vulnerabilities and Exposures (CVE) naming convention and that use the Open Vulnerability Assessment Language (OVAL) to determine/test for the presence of vulnerabilities. Suggested sources for vulnerability information include the Common Weakness Enumeration (CWE) listing and the National Vulnerability Database (NVD). In addition, security control assessments such as red team exercises provide other sources of potential vulnerabilities for which to scan. Organizations also consider using tools that express vulnerability impact by the Common Vulnerability Scoring System (CVSS). Related controls: CA-2, CA-7, CM-4, CM-6, RA- 2, RA-3, SA-11, SI-2.</p>

14. Security Assessment and Authorization (CA)

Control Number	CA-2
Title	Security Assessments
DHCS & CDSS	The organization must:

<p>Requirement</p>	<ul style="list-style-type: none"> a. Develops a security assessment plan that describes the scope of the assessment including: <ul style="list-style-type: none"> 1. Security controls and control enhancements under assessment; 2. Assessment procedures to be used to determine security control effectiveness; and 3. Assessment environment, assessment team, and assessment roles and responsibilities; b. Assesses the security controls in the information system and its environment of operation with organization-defined frequency to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security requirements; c. Produces a security assessment report that documents the results of the assessment; and d. Provides the results of the security control assessment to organization-defined individuals or roles.
<p>Supplemental Guidance (from NIST 800-53)</p>	<p>Organizations assess security controls in organizational information systems and the environments in which those systems operate as part of: (i) initial and ongoing security authorizations; (ii) FISMA annual assessments; (iii) continuous monitoring; and (iv) system development life cycle activities. Security assessments: (i) ensure that information security is built into organizational information systems; (ii) identify weaknesses and deficiencies early in the development process; (iii) provide essential information needed to make risk-based decisions as part of security authorization processes; and (iv) ensure compliance to vulnerability mitigation procedures. Assessments are conducted on the implemented security controls from Appendix F (main catalog) and Appendix G (Program Management controls) as documented in System Security Plans and Information Security Program Plans. Organizations can use other types of assessment activities such as vulnerability scanning and system monitoring to maintain the security posture of information systems during the entire life cycle. Security assessment reports document assessment results in sufficient detail as deemed necessary by organizations, to determine the accuracy and completeness of the reports and whether the security controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting security requirements. The FISMA requirement for assessing security controls at least annually does not require additional assessment activities to those activities already in place in organizational security authorization processes. Security assessment results are provided to the individuals or roles appropriate for the types of assessments being conducted. For example, assessments conducted in support of security authorization decisions are provided to authorizing officials or authorizing official designated representatives.</p> <p>To satisfy annual assessment requirements, organizations can use assessment results from the following sources: (i) initial or ongoing information system authorizations; (ii) continuous monitoring; or (iii) system development life cycle activities. Organizations ensure that security assessment results are current, relevant to the determination of security control effectiveness, and obtained with the appropriate level of assessor independence. Existing security control assessment results can be reused to the extent that the results are still valid and can also be supplemented with additional assessments as needed. Subsequent to initial authorizations and in accordance with OMB policy, organizations assess security controls during continuous monitoring. Organizations establish the frequency for ongoing security control assessments in accordance with organizational continuous monitoring strategies. Information Assurance Vulnerability Alerts provide useful examples of vulnerability mitigation procedures. External audits (e.g., audits by external entities such as regulatory agencies) are outside the scope of this control. Related controls: CA-5, CA-6, CA-7, PM-9, RA-5, SA-11, SA-12, SI-4.</p>

Control Number	CA-3
Title	System Interconnections
DHCS & CDSS Requirement	<p>The organization must:</p> <ul style="list-style-type: none"> a. Authorizes connections from the information system to other information systems through the use of Interconnection Security Agreements; b. Documents, for each interconnection, the interface characteristics, security requirements, and the nature of the information communicated; and c. Reviews and updates Interconnection Security Agreements [Assignment: organization-defined frequency].
Supplemental Guidance (from NIST 800-53)	<p>This control applies to dedicated connections between information systems (i.e., system interconnections) and does not apply to transitory, user-controlled connections such as email and website browsing. Organizations carefully consider the risks that may be introduced when information systems are connected to other systems with different security requirements and security controls, both within organizations and external to organizations. Authorizing officials determine the risk associated with information system connections and the appropriate controls employed. If interconnecting systems have the same authorizing official, organizations do not need to develop Interconnection Security Agreements. Instead, organizations can describe the interface characteristics between those interconnecting systems in their respective security plans. If interconnecting systems have different authorizing officials within the same organization, organizations can either develop Interconnection Security Agreements or describe the interface characteristics between systems in the security plans for the respective systems. Organizations may also incorporate Interconnection Security Agreement information into formal contracts, especially for interconnections established between federal agencies and nonfederal (i.e., private sector) organizations. Risk considerations also include information systems sharing the same networks. For certain technologies (e.g., space, unmanned aerial vehicles, and medical devices), there may be specialized connections in place during preoperational testing. Such connections may require Interconnection Security Agreements and be subject to additional security controls. Related controls: AC-3, AC-4, AC-20, AU-2, AU-12, AU-16, CA-7, IA-3, SA-9, SC-7, SI-4.</p>
Control Number	CA-7
Title	Continuous Monitoring
DHCS & CDSS Requirement	<p>The organization must develop a continuous monitoring strategy and implement a continuous monitoring program that includes:</p> <ul style="list-style-type: none"> a. Establishment of PII security controls to be monitored; c. Ongoing security control assessments in accordance with the organizational continuous monitoring strategy; d. Ongoing security status monitoring of PII security controls in accordance with the organizational continuous monitoring strategy; e. Correlation and analysis of security-related information generated by assessments and monitoring; f. Response actions to address results of the analysis of security-related information; and g. Reporting the security status of organization and the information system to organization-defined personnel or roles and to DHCS and CDSS when requested.

<p>Supplemental Guidance (from NIST 800-53)</p>	<p>Continuous monitoring programs facilitate ongoing awareness of threats, vulnerabilities, and information security to support organizational risk management decisions. The terms continuous and ongoing imply that organizations assess/analyze security controls and information security-related risks at a frequency sufficient to support organizational risk-based decisions. The results of continuous monitoring programs generate appropriate risk response actions by organizations. Continuous monitoring programs also allow organizations to maintain the security authorizations of information systems and common controls over time in highly dynamic environments of operation with changing mission/business needs, threats, vulnerabilities, and technologies. Having access to security-related information on a continuing basis through reports/dashboards gives organizational officials the capability to make more effective and timely risk management decisions, including ongoing security authorization decisions. Automation supports more frequent updates to security authorization packages, hardware/software/firmware inventories, and other system information. Effectiveness is further enhanced when continuous monitoring outputs are formatted to provide information that is specific, measurable, actionable, relevant, and timely. Continuous monitoring activities are scaled in accordance with the security categories of information systems. Related controls: CA-2, CA-5, CA-6, CM-3, CM-4, PM-6, PM-9, RA-5, SA- 11, SA-12, SI-2, SI-4.</p>
<p>Control Number</p>	<p>CA-8</p>
<p>Title</p>	<p>Penetration Testing</p>
<p>DHCS & CDSS Requirement</p>	<p>The organization must conduct penetration testing annually on systems storing, processing, or transmitting PII.</p>
<p>Supplemental Guidance (from NIST 800-53)</p>	<p>Penetration testing is a specialized type of assessment conducted on information systems or individual system components to identify vulnerabilities that could be exploited by adversaries. Such testing can be used to either validate vulnerabilities or determine the degree of resistance organizational information systems have to adversaries within a set of specified constraints (e.g., time, resources, and/or skills). Penetration testing attempts to duplicate the actions of adversaries in carrying out hostile cyber-attacks against organizations and provides a more in- depth analysis of security-related weaknesses/deficiencies. Organizations can also use the results of vulnerability analyses to support penetration testing activities. Penetration testing can be conducted on the hardware, software, or firmware components of an information system and can exercise both physical and technical security controls. A standard method for penetration testing includes, for example:</p> <ul style="list-style-type: none"> (i) pretest analysis based on full knowledge of the target system; (ii) pretest identification of potential vulnerabilities based on pretest analysis; and (iii) testing designed to determine exploitability of identified vulnerabilities. All parties agree to the rules of engagement before the commencement of penetration testing scenarios. Organizations correlate the penetration testing rules of engagement with the tools, techniques, and procedures that are anticipated to be employed by adversaries carrying out attacks. Organizational risk assessments guide decisions on the level of independence required for personnel conducting penetration testing. Related control: SA-12.

15. System and Communications Protection (SC)

Control Number	SC-7
Title	Boundary Protection
DHCS & CDSS Requirement	<p>The organization information system must:</p> <ul style="list-style-type: none"> a. Monitor and control communications at the external boundary of the system and at key internal boundaries within the system; b. Implements subnetworks for publicly accessible system components that are physically and logically separated from internal organizational networks; and c. Connect to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.
Supplemental Guidance (from NIST 800-53)	<p>Managed interfaces include, for example, gateways, routers, firewalls, guards, network-based malicious code analysis and virtualization systems, or encrypted tunnels implemented within a security architecture (e.g., routers protecting firewalls or application gateways residing on protected subnetworks). Subnetworks that are physically or logically separated from internal networks are referred to as demilitarized zones or DMZs. Restricting or prohibiting interfaces within organizational information systems includes, for example, restricting external web traffic to designated web servers within managed interfaces and prohibiting external traffic that appears to be spoofing internal addresses. Organizations consider the shared nature of commercial telecommunications services in the implementation of security controls associated with the use of such services. Commercial telecommunications services are commonly based on network components and consolidated management systems shared by all attached commercial customers, and may also include third party-provided access lines and other service elements.</p> <p>Such transmission services may represent sources of increased risk despite contract security provisions. Related controls: AC-4, AC-17, CA-3, CM-7, CP-8, IR-4, RA-3, SC-5, SC-13.</p>
Control Number	SC-8
Title	Transmission Confidentiality and Integrity
DHCS & CDSS Requirement	<p>The organization information system must: Protect the confidentiality of transmitted information.</p>
Supplemental Guidance (from NIST 800-53)	<p>This control applies to both internal and external networks and all types of information system components from which information can be transmitted (e.g., servers, mobile devices, notebook computers, printers, copiers, scanners, facsimile machines). Communication paths outside the physical protection of a controlled boundary are exposed to the possibility of interception and modification. Protecting the confidentiality and/or integrity of organizational information can be accomplished by physical means (e.g., by employing protected distribution systems) or by logical means (e.g., employing encryption techniques). Organizations relying on commercial providers offering transmission services as commodity services rather than as fully dedicated services (i.e., services which can be highly specialized to individual customer needs), may find it difficult to obtain the necessary assurances regarding the implementation of needed security controls for transmission confidentiality/integrity. In such situations, organizations determine what types of confidentiality/integrity services are available in standard, commercial telecommunication service packages. If it is infeasible or impractical to obtain the necessary security controls and assurances of control effectiveness through appropriate contracting vehicles, organizations implement appropriate compensating security controls or explicitly accept the additional risk.</p>

	Related controls: AC-17, PE-4.
Control Number	SC-8(1)
Title	Transmission Confidentiality and Integrity Cryptographic or Alternate Physical Protection
DHCS & CDSS Requirement	The organization information system must implement cryptographic mechanisms to prevent unauthorized disclosure of information during transmission.
Supplemental Guidance (from NIST 800-53)	Encrypting information for transmission protects information from unauthorized disclosure and modification. Cryptographic mechanisms implemented to protect information integrity include, for example, cryptographic hash functions which have common application in digital signatures, checksums, and message authentication codes. Alternative physical security safeguards include, for example, protected distribution systems. Related control: SC-13.
Control Number SC-13	Control Number SC-13
Title	Cryptographic Protection
CDSS Requirement	The organization information system must implement FIPS 140-3 compliant encryption modules in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.
Supplemental Guidance (from NIST 800-53)	Cryptography can be employed to support a variety of security solutions including, for example, the protection of classified and Controlled Unclassified Information, the provision of digital signatures, and the enforcement of information separation when authorized individuals have the necessary clearances for such information but lack the necessary formal access approvals. Cryptography can also be used to support random number generation and hash generation. Generally applicable cryptographic standards include FIPS-validated cryptography and NSA-approved cryptography. This control does not impose any requirements on organizations to use cryptography. However, if cryptography is required based on the selection of other security controls, organizations define each type of cryptographic use and the type of cryptography required (e.g., protection of classified information: NSA-approved cryptography; provision of digital signatures: FIPS-validated cryptography). Related controls: AC-2, AC-3, AC-7, AC-17, AC-18, AU-9, AU-10, CM-11, CP-9, IA-3, IA-7, MA-4, MP-2, MP-4, MP-5, SA-4, SC-8, SC-12, SC-28, SI-7.
Control Number	SC-28
Title	Protection of Information at Rest
DHCS & CDSS Requirement	The organization information system must: Protect the confidentiality of PII at rest.
Supplemental Guidance (from NIST 800-53)	This control addresses the confidentiality and integrity of information at rest and covers user information and system information. Information at rest refers to the state of information when it is located on storage devices as specific components of information systems. System-related information requiring protection includes, for example, configurations or rule sets for firewalls, gateways, intrusion detection/prevention systems, filtering routers, and authenticator content. Organizations may employ different mechanisms to achieve confidentiality and integrity protections, including the use of cryptographic mechanisms and file share scanning. Integrity protection can be achieved, for example, by implementing Write-Once-Read-Many (WORM) technologies. Organizations may also employ other security controls including, for example,

	secure off-line storage in lieu of online storage when adequate protection of information at rest cannot otherwise be achieved and/or continuous monitoring to identify malicious code at rest. Related controls: AC-3, AC-6, CA-7, CM-3, CM-5, CM-6, PE-3, SC-8, SC-13, SI-3, SI-7.
--	--

16. System and Information Integrity (SI)

Control Number	SI-2
Title	Flaw Remediation
DHCS & CDSS Requirement	<p>The organization must:</p> <ul style="list-style-type: none"> a. Identify, report, and correct information system flaws; b. Tests software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation; c. Installs security-relevant software and firmware updates, within acceptable organization standards, of the release of the updates; and d. Incorporates flaw remediation into the organizational configuration management process.
Supplemental Guidance (from NIST 800-53)	<p>Organizations identify information systems affected by announced software flaws including potential vulnerabilities resulting from those flaws, and report this information to designated organizational personnel with information security responsibilities. Security-relevant software updates include, for example, patches, service packs, hot fixes, and anti-virus signatures.</p> <p>Organizations also address flaws discovered during security assessments, continuous monitoring, incident response activities, and system error handling. Organizations take advantage of available resources such as the Common Weakness Enumeration (CWE) or Common Vulnerabilities and Exposures (CVE) databases in remediating flaws discovered in organizational information systems. By incorporating flaw remediation into ongoing configuration management processes, required/anticipated remediation actions can be tracked and verified. Flaw remediation actions that can be tracked and verified include, for example, determining whether organizations follow US-CERT guidance and Information Assurance Vulnerability Alerts. Organization-defined time periods for updating security-relevant software and firmware may vary based on a variety of factors including, for example, the security category of the information system or the criticality of the update (i.e., severity of the vulnerability related to the discovered flaw). Some types of flaw remediation may require more testing than other types. Organizations determine the degree and type of testing needed for the specific type of flaw remediation activity under consideration and also the types of changes that are to be configuration-managed. In some situations, organizations may determine that the testing of software and/or firmware updates is not necessary or practical, for example, when implementing simple anti-virus signature updates. Organizations may also consider in testing decisions, whether security-relevant software or firmware updates are obtained from authorized sources with appropriate digital signatures. Related controls: CA-2, CA-7, CM-3, CM-5, CM-8, MA-2, IR-4, RA-5, SA-10, SA-11, SI-11.</p>
Control Number	SI-3
Title	Malicious Code Protection
DHCS & CDSS Requirement	<p>The organization must:</p> <ul style="list-style-type: none"> a. Employ malicious code protection mechanisms at information system entry and exit

	<p>points to detect and eradicate malicious code;</p> <ul style="list-style-type: none"> b. Update malicious code protection mechanisms whenever new releases are available in accordance with organizational configuration management policy and procedures; c. Configure malicious code protection mechanisms to: <ul style="list-style-type: none"> 1. Perform periodic scans of the information system and real-time scans of files from external sources at the endpoint and network entry/exit points as the files are downloaded, opened, or executed in accordance with organizational security policy; and 2. Block malicious code or quarantine malicious code, and send alert to administrator for incident handling in response to malicious code detection; and d. Address the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system
<p>Supplemental Guidance (from NIST 800-53)</p>	<p>Information system entry and exit points include, for example, firewalls, electronic mail servers, web servers, proxy servers, remote-access servers, workstations, notebook computers, and mobile devices. Malicious code includes, for example, viruses, worms, Trojan horses, and spyware. Malicious code can also be encoded in various formats (e.g., UUENCODE, Unicode), contained within compressed or hidden files, or hidden in files using steganography. Malicious code can be transported by different means including, for example, web accesses, electronic mail, electronic mail attachments, and portable storage devices. Malicious code insertions occur through the exploitation of information system vulnerabilities. Malicious code protection mechanisms include, for example, anti-virus signature definitions and reputation-based technologies. A variety of technologies and methods exist to limit or eliminate the effects of malicious code. Pervasive configuration management and comprehensive software integrity controls may be effective in preventing execution of unauthorized code. In addition to commercial off-the-shelf software, malicious code may also be present in custom-built software. This could include, for example, logic bombs, back doors, and other types of cyber attacks that could affect organizational missions/business functions. Traditional malicious code protection mechanisms cannot always detect such code. In these situations, organizations rely instead on other safeguards including, for example, secure coding practices, configuration management and control, trusted procurement processes, and monitoring practices to help ensure that software does not perform functions other than the functions intended. Organizations may determine that in response to the detection of malicious code, different actions may be warranted. For example, organizations can define actions in response to malicious code detection during periodic scans, actions in response to detection of malicious downloads, and/or actions in response to detection of maliciousness when attempting to open or execute files.</p> <p>Related controls: CM-3, MP-2, SA-4, SA-8, SA-12, SA-13, SC-7, SC-26, SC-44, SI-2, SI-4, SI-7.</p>
<p>Control Number</p>	<p>SI-4</p>
<p>Title</p>	<p>Information System Monitoring</p>
<p>DHCS & CDSS Requirement</p>	<p>The organization must:</p> <ul style="list-style-type: none"> a. Monitor the information system to detect: <ul style="list-style-type: none"> 1. Attacks and indicators of potential attacks in accordance with organization-defined monitoring objectives; and 2. Unauthorized local, network, and remote connections;

	<ul style="list-style-type: none"> b. Identify unauthorized use of the information system through organization-defined techniques and methods; c. Deploy monitoring devices: <ul style="list-style-type: none"> 1. Strategically within the information system to collect organization-determined essential information; and 2. At ad hoc locations within the system to track specific types of transactions of interest to the organization; d. Protect information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion; e. Heighten the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations and assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information; Relevant risk would apply to anything impacting the confidentiality integrity or availability of the information system. f. Obtain legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations; and g. Provides organization-defined information system monitoring information to organization- defined personnel and DHCS and CDSS as needed.
<p>Supplemental Guidance (from NIST 800-53)</p>	<p>Information system monitoring includes external and internal monitoring. External monitoring includes the observation of events occurring at the information system boundary (i.e., part of perimeter defense and boundary protection). Internal monitoring includes the observation of events occurring within the information system. Organizations can monitor information systems, for example, by observing audit activities in real time or by observing other system aspects such as access patterns, characteristics of access, and other actions. The monitoring objectives may guide determination of the events. Information system monitoring capability is achieved through a variety of tools and techniques (e.g., intrusion detection systems, intrusion prevention systems, malicious code protection software, scanning tools, audit record monitoring software, network monitoring software). Strategic locations for monitoring devices include, for example, selected perimeter locations and near server farms supporting critical applications, with such devices typically being employed at the managed interfaces associated with controls SC-7 and AC-17. Einstein network monitoring devices from the Department of Homeland Security can also be included as monitoring devices. The granularity of monitoring information collected is based on organizational monitoring objectives and the capability of information systems to support such objectives. Specific types of transactions of interest include, for example, Hyper Text Transfer Protocol (HTTP) traffic that bypasses HTTP proxies. Information system monitoring is an integral part of organizational continuous monitoring and incident response programs. Output from system monitoring serves as input to continuous monitoring and incident response programs. A network connection is any connection with a device that communicates through a network (e.g., local area network, Internet). A remote connection is any connection with a device communicating through an external network (e.g., the Internet). Local, network, and remote connections can be either wired or wireless. Related controls: AC-3, AC-4, AC-8, AC-17, AU-2, AU-6, AU-7, AU-9, AU-12, CA-7, IR-4, PE-3, RA-5, SC-7, SC-26, SC-35, SI-3, SI-7.</p>
<p>Control Number</p>	<p>SI-4(5)</p>

Title	Information System Monitoring System Generated Alerts
DHCS & CDSS Requirement	<p>The information system alerts County Worker when the following indications of compromise or potential compromise occur. County will notify Contractor as needed.</p> <ol style="list-style-type: none"> 1. Protected system files or directories have been modified without notification from the appropriate change/configuration management channels. 2. System performance indicates resource consumption that is inconsistent with expected operating conditions. 3. Auditing functionality has been disabled or modified to reduce audit visibility. 4. Audit or log records have been deleted or modified without explanation. 5. The system is raising alerts or faults in a manner that indicates the presence of an abnormal condition. 6. Resource or service requests are initiated from clients that are outside of the expected client membership set. 7. The system reports failed logins or password changes for administrative or key service accounts. 8. Processes and services are running that are outside of the baseline system profile. 9. Utilities, tools, or scripts have been saved or installed on production systems without clear indication of their use or purpose.
Supplemental Guidance (from NIST 800-53)	Alerts may be generated from a variety of sources, including, for example, audit records or inputs from malicious code protection mechanisms, intrusion detection or prevention mechanisms, or boundary protection devices such as firewalls, gateways, and routers. Alerts can be transmitted, for example, telephonically, by electronic mail messages, or by text messaging. Organizational personnel on the notification list can include, for example, system administrators, mission/business owners, system owners, or information system security officers. Related controls: AU-5, PE-6.
Control Number	SI-4(13)
Title	Information System Monitoring Analyze Traffic / Event Patterns
DHCS & CDSS Requirement	<p>The organization must:</p> <ol style="list-style-type: none"> a. Analyzes communications traffic/event patterns for the information system; b. Develops profiles representing common traffic patterns and/or events; and c. Uses the traffic/event profiles in tuning system-monitoring devices to reduce the number of false positives and the number of false negatives.
Supplemental Guidance (from NIST 800-53)	None

17. System and Services Acquisition (SA)

Control Number	SA-9
Title	External Information System Services
DHCS & CDSS	The organization must:

<p>Requirement</p>	<p>a. Require that providers of external information system services comply with organizational information security requirements and employ organization-defined security controls in accordance with DHCS and CDSS PSA, applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance;</p> <p>b. Defines and documents government oversight and user roles and responsibilities with regard to external information system services; and</p> <p>c. Employs organization-defined processes, methods, and techniques to monitor security control compliance by external service providers on an ongoing basis.</p> <p><i>The state organization will provide its contractors and agents with copies of the Agreement, related IEAs, and all related attachments before initial disclosure of PII to such contractors and agents. Prior to signing the Agreement, and thereafter at DHCS's and CDSS's request, the state organization will obtain from its contractors and agents a current list of the employees of such contractors and agents with access to PII and provide such lists to DHCS and CDSS.</i></p>
<p>Supplemental Guidance (from NIST 800-53)</p>	<p>External information system services are services that are implemented outside of the authorization boundaries of organizational information systems. This includes services that are used by, but not a part of, organizational information systems. FISMA and OMB policy require that organizations using external service providers that are processing, storing, or transmitting federal information or operating information systems on behalf of the federal government ensure that such providers meet the same security requirements that federal agencies are required to meet. Organizations establish relationships with external service providers in a variety of ways including, for example, through joint ventures, business partnerships, contracts, interagency agreements, lines of business arrangements, licensing agreements, and supply chain exchanges. The responsibility for managing risks from the use of external information system services remains with authorizing officials. For services external to organizations, a chain of trust requires that organizations establish and retain a level of confidence that each participating provider in the potentially complex consumer-provider relationship provides adequate protection for the services rendered. The extent and nature of this chain of trust varies based on the relationships between organizations and the external providers. Organizations document the basis for trust relationships so the relationships can be monitored over time. External information system services documentation includes government, service providers, end user security roles and responsibilities, and service-level agreements. Service-level agreements define expectations of performance for security controls, describe measurable outcomes, and identify remedies and response requirements for identified instances of noncompliance. Related controls: CA-3, IR-7, PS-7.</p>
<p>Control Number</p>	<p>SA-11</p>
<p>Title</p>	<p>Developer Security Testing And Evaluation</p>
<p>DHCS & CDSS Requirement</p>	<p>The organization must require the developer of the information system, system component, or information system service to:</p> <p>a. Create and implement a security assessment plan;</p> <p>b. Perform [Selection (one or more): unit; integration; system; regression] testing/evaluation at [Assignment: organization-defined depth and coverage];</p> <p>c. Produce evidence of the execution of the security assessment plan and the results of the security testing/evaluation;</p> <p>d. Implement a verifiable flaw remediation process; and</p>

<p>Supplemental Guidance (from NIST 800-53)</p>	<p>e. Correct flaws identified during security testing/evaluation</p> <p>Supplemental Guidance: Developmental security testing/evaluation occurs at all post-design phases of the system development life cycle. Such testing/evaluation confirms that the required security controls are implemented correctly, operating as intended, enforcing the desired security policy, and meeting established security requirements. Security properties of information systems may be affected by the interconnection of system components or changes to those components. These interconnections or changes (e.g., upgrading or replacing applications and operating systems) may adversely affect previously implemented security controls. This control provides additional types of security testing/evaluation that developers can conduct to reduce or eliminate potential flaws. Testing custom software applications may require approaches such as static analysis, dynamic analysis, binary analysis, or a hybrid of the three approaches. Developers can employ these analysis approaches in a variety of tools (e.g., web-based application scanners, static analysis tools, binary analyzers) and in source code reviews. Security assessment plans provide the specific activities that developers plan to carry out including the types of analyses, testing, evaluation, and reviews of software and firmware components, the degree of rigor to be applied, and the types of artifacts produced during those processes. The depth of security testing/evaluation refers to the rigor and level of detail associated with the assessment process (e.g., black box, gray box, or white box testing). The coverage of security testing/evaluation refers to the scope (i.e., number and type) of the artifacts included in the assessment process. Contracts specify the acceptance criteria for security assessment plans, flaw remediation processes, and the evidence that the plans/processes have been diligently applied. Methods for reviewing and protecting assessment plans, evidence, and documentation are commensurate with the security category or classification level of the information system. Contracts may specify documentation protection requirements. Related controls: CA-2, CM-4, SA-3, SA-4, SA-5, SI-2.</p>
--	--

B. *Minimum Cloud Security Requirements*

Contractor and any agents, subcontractors, and vendors storing PII in a cloud service must comply with the Cloud Computing Policy, State Administration Manual (SAM) Sections 4983-4983.1, and employ the capabilities in the Cloud Security Standard, SIMM 5315-B to protect information and systems in cloud services as outlined below.

1. Identify and classify assets to focus and prioritize efforts in aligning business needs and risk management.
2. Each information asset for which the Contractor entity has ownership responsibility shall be inventoried and identified to include the following:
 - a. Description and value of the information asset.
 - b. Owner of the information asset.
 - c. Custodians of the information asset.
 - d. Users of the information asset.
 - e. Classification of information.
 - f. [FIPS Publication 199](#) categorization and level of protection (Low, Moderate, or High).
 - g. Importance of information assets to the execution of the Agency/state entity’s mission and program function.

- h. Potential consequences and impacts if confidentiality, integrity, and availability of the information asset were compromised.
3. Security of cloud services stems from managing authentication and fine-grained authorization. To safeguard cloud systems, Contractor shall establish processes and procedures to ensure:
 - a. Maintenance of user identities, including both provisioning and de-provisioning;
 - b. Enforcement of password policies or more advanced multifactor mechanisms to authenticate users and devices;
 - c. Management of access control rules, limiting access to the minimum necessary to complete defined responsibilities;
 - d. Separation of duties to avoid functional conflicts;
 - e. Periodic recertification of access control rules to identify those that are no longer needed or provide overly broad clearance;
 - f. Use of privileged accounts that can bypass security are restricted and audited;
 - g. Systems to administer access based on roles are defined and installed; and
 - h. Encryption keys and system security certificates are effectively generated, exchanged, stored and safeguarded.
 4. Infrastructure protection controls limit the impact of unintended access or potential vulnerabilities. PaaS and SaaS resources may already have these controls implemented by the service provider. Contractor must configure information assets to provide only essential capabilities.
 5. Contractor is entrusted with protecting the integrity and confidentiality of data processed by their information systems. Cloud technologies simplify data protection by providing managed data storage services with native protection and backup features, but these features must be configured and managed appropriately.
 6. Detective controls identify potential security threats or incidents, supporting timely investigation and response. Contractor must continuously identify and remediate vulnerabilities.
 7. Response controls enable timely event and incident response which is essential to reducing the impact if an incident were to occur. Compliance with incident management requirements as outlined in VII. Notification and Investigation of Breaches and Security Incidents.
 8. Recover controls facilitate long-term recovery activities following events or incidents. With cloud services, primarily SaaS solutions, the services provider hosts the data in its application, and unless properly planned and provisioned for in the contract with the service provider it may be difficult or impossible to obtain the data in a usable format at contract termination. Contractor must ensure agreements with cloud service providers include recover controls.
- C. **Minimum Necessary.** Only the minimum necessary amount of PII required to perform required business functions applicable to the terms of this Agreement may be used, disclosed, copied, downloaded, or exported.
- D. **Transmission and Storage of PII.** All persons that will be working with PII shall employ FIPS 140-2 or greater approved security functions as described in section 6.2.2 of NIST SP 800-140Cr1 encryption of PII at rest and in motion unless Contractor determines it is

not reasonable and appropriate to do so based upon a risk assessment, and equivalent alternative measures are in place and documented as such. In addition, Contractor shall maintain, at a minimum, the most current industry standards for transmission and storage of County of Orange data and other confidential information.

- E. ***DHCS Remote Work Policy.*** Contractor, its Contractor Workers and any agents, subcontractors, and vendors accessing PII pursuant to this PSA when working remotely, shall follow reasonable policies and procedures that are equivalent to or better than the DHCS Remote Work Policy, as published in [Medi-Cal Eligibility Division Informational Letter \(MEDIL\) | 23-35E](#). Working remotely means working from a physical location not under the control of the person's employer.

If DHCS changes the terms of the DHCS Remote to Work Policy, DHCS will, as soon as reasonably possible, supply copies to the County of Orange or its designee as well as DHCS' proposed target date for compliance. For a period of thirty (30) days, DHCS will accept input from the County of Orange or its designee on the proposed changes. DHCS will issue a new policy in a future MEDIL. If the Contractor is unable to comply with these standards, the Contractor will be asked to develop a Plan of Action and Milestones (POA&M) detailing a concrete roadmap to becoming fully compliant with the policy's standard. The POA&M must be provided to the County of Orange for review and approval. Any Contractor who is under a POA&M will be required to provide quarterly updates to the County of Orange until the fully compliant.

VI. AUDIT CONTROLS

- A. ***Audit Control Mechanisms.*** The Contractor shall ensure audit control mechanisms are in place that are compliant with the Technical Security Controls within Section V of this Agreement.
- B. ***Anomalies.*** When the Contractor or the County of Orange suspects MEDS usage anomalies, the Contractor shall work with the County of Orange to investigate the anomalies and report conclusions of such investigations and remediation to the County of Orange.
- C. ***Notification to the County of Orange in event Contractor is subject to other Audit.*** If Contractor is the subject of an audit, compliance review, investigation, or any proceeding that is related to the performance of its obligations pursuant to this Agreement, or is the subject of any judicial or administrative proceeding alleging a violation of law related to the privacy and security of PII, including but not limited to Medi-Cal PII, the Contractor shall promptly notify the County of Orange unless it is legally prohibited from doing so.

VII. PAPER, RECORD, AND MEDIA CONTROLS

- A. ***Supervision of Data.*** PII shall not be left unattended at any time, unless it is locked in a file cabinet, file room, desk or office at the individual's place of employment or at home when working remotely. Unattended means that information may be observed by an individual not authorized to access the information.
- B. ***Data in Vehicles.*** The Contractor shall have policies that include, based on applicable risk factors, a description of the circumstances under which the Contractor Workers can transport PII, as well as the physical security requirements during transport. A Contractor that chooses to permit its Contractor Workers to leave records unattended in vehicles, shall

include provisions in its policies to provide that the PII is stored in a non-visible area such as a trunk, that the vehicle is locked, and that under no circumstances permit PII to be left unattended in a vehicle overnight or for other extended periods of time.

- C. **Public Modes of Transportation.** PII shall not be left unattended at any time in airplanes, buses, trains, etc., inclusive of baggage areas. This should be included in training due to the nature of the risk.
- D. **Escorting Visitors.** Visitors to areas where PII is contained shall be escorted, and PII shall be kept out of sight while visitors are in the area.
- E. **Confidential Destruction.** PII shall be disposed of through confidential means, such as cross cut shredding or pulverizing.
- F. **Removal of Data.** PII shall not be removed from the premises of Contractor except for justifiable business purposes.
- G. **Faxing.**
 - 1. Faxes containing PII shall not be left unattended and fax machines shall be in secure areas.
 - 2. Faxes shall contain a confidentiality statement notifying persons receiving faxes in error to destroy them and notify the sender.
 - 3. Fax numbers shall be verified with the intended recipient before sending the fax.
- H. **Mailing.**
 - 1. Mailings containing PII shall be sealed and secured from damage or inappropriate viewing of PII to the extent possible.
 - 2. Mailings that include 500 or more individually identifiable records containing PII in a single package shall be sent using a tracked mailing method that includes verification of delivery and receipt.

VIII. NOTIFICATION AND INVESTIGATION OF BREACHES AND SECURITY INCIDENTS

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

A. **Initial Notice to the County of Orange:**

The Contractor shall notify the County of Orange using County online incident reporting portal of any suspected security incident, intrusion, or unauthorized access, use, or disclosure of PII or potential loss of PII. When making notification, the following applies:

- 1. If a suspected security incident involves PII provided or verified by SSA, the Contractor shall immediately notify the County of Orange upon discovery. For more information on SSA data, please see the Definition section of this Agreement.
- 2. If a suspected security incident does not involve PII provided or verified by SSA, the Contractor shall notify the County of Orange promptly and in no event later than one working day of discovery of:

- a. Unsecured PII if the PII is reasonably believed to have been accessed or acquired by an unauthorized person;
- b. Any suspected security incident which risks unauthorized access to PII and/or;
- c. Any intrusion or unauthorized access, use, or disclosure of PII in violation of this Agreement; or
- d. Potential loss of PII affecting this Agreement.

Notice to County shall include all information known at the time the incident is reported. Contractor shall submit notice via the link [County of Orange Incident Reporting Portal](#) and email contact using the information listed in subsection H..

If County online incident reporting portal is unavailable, notice to County can instead be made via email using the County Privacy Incident Report (PIR) form, which the County will coordinate with Contractor.

A breach shall be treated as discovered by the Contractor as of the first day on which the breach is known, or by exercising reasonable diligence would have been known, to any person (other than the person committing the breach), who is an employee, officer or other agent of the Contractor.

Upon discovery of a breach, security incident, intrusion, or unauthorized access, use, or disclosure of PII, the Contractor shall take:

1. Prompt corrective action to mitigate any risks or damages involved with the security incident or breach; and
 2. Any action pertaining to such unauthorized disclosure required by applicable Federal and State laws and regulations.
- B. **Investigation of Security Incident or Breach.** The Contractor shall immediately investigate such a security incident, breach, or unauthorized use of PII.
- C. **Complete Report.** Within ten (10) working days of the discovery the Contractor shall provide any additional information related to the incident requested by the County of Orange. The Contractor shall make reasonable efforts to provide the County of Orange with such information.

The complete report must include an assessment of all known factors relevant to a determination of whether a breach occurred under applicable federal and state laws. The report shall include a full, detailed corrective action plan (CAP) including mitigating measures that were taken to halt and/or contain the improper use or disclosure.

If the County of Orange requests additional information related to the incident, the Contractor shall make reasonable efforts to provide the County of Orange with such information. If necessary, the Contractor shall submit an updated report with revisions and/or additional information after the Completed Report has been provided. The County of Orange will review and determine whether a breach occurred and whether individual notification is required. The County of Orange will maintain the final decision making over a breach determination.

- D. **Notification of Individuals.** If the cause of a breach is solely attributable to the Contractor or its agents, Contractor shall notify individuals accordingly and shall pay all costs of such notifications as well as any costs associated with the breach. The notifications shall comply

with applicable federal and state law. The County of Orange and DHCS shall approve the time, manner, and content of any such notifications and their review and approval must be obtained before the notifications are made. The County of Orange and the Contractor shall work together to ensure that notification of individuals is done in compliance with statutory deadlines within applicable federal and state law.

If the cause of a breach is solely attributable to the County of Orange, the County of Orange shall pay all costs of such notifications as well as any costs associated with the breach. If there is any question as to whether the County of Orange or the Contractor is responsible for the breach or the County of Orange and the Contractor acknowledge that both are responsible for the breach, the County of Orange and the Contractor shall jointly determine responsibility for purposes of allocating the costs.

1. All notifications (regardless of breach status) regarding beneficiaries' PII shall comply with the requirements set forth in Section 1798.29 of the California Civil Code and Section 17932 of Title 42 of United States Code, inclusive of its implementing regulations, including but not limited to the requirement that the notifications be made without unreasonable delay and in no event later than **sixty (60) calendar days** from discovery.

E. *Responsibility for Reporting of Breaches*

1. ***Breach Attributable to Contractor.*** If the cause of a breach of PII is attributable to the Contractor or its agents, subcontractors, or vendors, the Contractor shall be responsible for all required reporting of the breach.
2. ***Breach Attributable to the County of Orange.*** If the cause of the breach is attributable to the County of Orange, the County of Orange shall be responsible for all required reporting of the breach.

F. *Coordination of Reporting.* When applicable law requires the breach be reported to a federal or state agency, or that notice be given to media outlets, the County of Orange and the Contractor shall coordinate to ensure such reporting is compliant with applicable law and prevent duplicate reporting and to jointly determine responsibility for purposes of allocating the costs of such reports, if any.

G. *Submission of Sample Notification to Attorney General:* If the cause of the breach is attributable to the Contractor or an agent, subcontractor, or vendor of the Contractor and if notification to more than 500 individuals is required pursuant to California Civil Code section 1798.29, regardless of whether Contractor is considered only a custodian and/or non-owner of the PII, Contractor shall, at its sole expense and at the sole election of the County of Orange, either:

1. Electronically submit a single sample copy of the security breach notification, excluding any personally identifiable information, to the Attorney General pursuant to the format, content, and timeliness provisions of Section 1798.29, subdivision (e). Contractor shall inform the County of Orange Privacy Officer of the time, manner, and content of any such submissions prior to the transmission of such submissions to the Attorney General; or
2. Cooperate with and assist the County of Orange in its submission of a sample copy of the notification to the Attorney General.

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

County of Orange Breach and Security Incident Reporting	
<p>Andrew Alipanah, MBA, CISSP Chief Information Security Officer County of Orange Enterprise Privacy & Cybersecurity</p> <p>721 S. Parker St., Ste. 200 Orange, CA 92868</p> <p>Email: Andrew.Alipanah@ocit.oc.gov</p> <p>Telephone: (714) 567-7611</p>	<p>Linda Le, CHC, CHPC, CHP County Privacy Officer County of Orange Enterprise Privacy & Cybersecurity</p> <p>721 S. Parker St., Suite 200 Orange, CA 92868</p> <p>Email: privacyofficer@ocgov.com securityadmin@ocit.oc.gov linda.le@ocit.oc.gov</p> <p>Telephone: (714) 834-4082</p>
<p>Karen Vu Procurement Contract Manager, Senior Contracts Services</p> <p>County of Orange Social Services Agency 500 N. State College Blvd. Orange, CA 92868 Email: Karen.vu@ssa.ocgov.com</p> <p>Telephone: 714-541-7785</p>	<p>Alin Buna Procurement Contract Manager, Senior Procurement Services</p> <p>County of Orange Social Services Agency 500 N. State College Blvd. Orange, CA 92868 Email: Alin.buna@ssa.ocgov.com</p> <p>Telephone: 714-541-7767</p>
<p><i>The preferred method of communication is email, when available. Do not include any PII unless requested by the County of Orange.</i></p>	

IX. RESERVED

The Contractor shall utilize the below contact information for any PSA-related inquiries or questions. The County of Orange reserves the right to make changes to the contact information by giving written notice to the Contractor. Said changes shall not require an amendment to this Agreement or any other agreement into which it is incorporated. *Please use the contact information listed in Section X of this Agreement for any PII incident or breach reporting.*

PSA Inquiries and Questions
 County of Orange Social Services Agency
 500 N. State College Blvd.
 Orange, CA 92868

 Email: ssacontractsservices@ssa.ocgov.com

X. COMPLIANCE WITH SSA AGREEMENT

The Contractor agrees to comply with applicable privacy and security requirements in the Computer Matching and Privacy Protection Act Agreement (CMPPA) between SSA and the California Health and Human Services Agency (CalHHS), in the Information Exchange Agreement (IEA) between SSA and DHCS and CDSS, and in the Electronic Information Exchange Security Requirements and Procedures for State and Local Agencies Exchanging Electronic Information with SSA (TSSR), which are incorporated into this Agreement within section V. Technical Security Controls and Exhibit A (available upon request).

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

If SSA changes the terms of its agreement(s) with DHCS and CDSS, the County of Orange will, as soon as reasonably possible after receipt from DHCS and CDSS, supply copies to the Contractor as well as DHCS’ and CDSS’ proposed target date for compliance. Once a target date for compliance is determined by SSA, the County of Orange will supply copies of the changed agreement to the Contractor after receipt from DHCS and CDSS, along with the compliance date expected by SSA. If the Contractor is not able to meet the SSA compliance date, the Contractor will be asked to develop a POA&M detailing a concrete roadmap to becoming fully compliant with the policy’s standard. The POA&M must be provided to the County of Orange for review and approval. Any Contractor who is under a POA&M will be required to provide quarterly updates to the County of Orange until the fully compliant.

A copy of Exhibit A can be requested by the Contractor from the County of Orange using the contact information listed in Section VIII.H of this Agreement.

XI. COMPLIANCE WITH DEPARTMENT OF HOMELAND SECURITY AGREEMENT

The Contractor agrees to comply with substantive privacy and security requirements in the Computer Matching Agreement (CMA) between the Department of Homeland Security, United States Citizenship and Immigration Services (DHS-USCIS), DHCS and CDSS, which is hereby incorporated into this Agreement (Exhibit B) and available upon request. If there is any conflict between a privacy and security standard in the CMA and a standard in this Agreement, the most stringent standard shall apply. The most stringent standard means the standard which provides the greatest protection to PII.

If DHS-USCIS changes the terms of its agreement(s) with DHCS and CDSS, the County of Orange will, as soon as reasonably possible after receipt from DHCS and CDSS, supply copies to the Contractor as well as DHCS’ and CDSS’ proposed target date for compliance. Once a target date for compliance is determined by DHS-USCIS, the County of Orange will supply copies of the

changed agreement to Contractor after receipt from DHCS and CDSS, along with the compliance date expected by DHS-USCIS. If the Contractor is not able to meet the DHS-USCIS compliance date, the POA&M must be provided to the County of Orange for review and approval. Any Contractor who is under a POA&M will be required to provide quarterly updates to the County of Orange until the fully compliant.

A copy of Exhibit B can be requested by the Contractor from the County of Orange using the contact information listed in Section VIII.H of this Agreement.

XII. CONTRACTOR'S AGENTS, SUBCONTRACTORS, AND VENDORS

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

Contractors who would like assistance or guidance with this requirement are encouraged to coordinate with the County of Orange.

XIII. ASSESSMENTS AND REVIEWS

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

XIV. ASSISTANCE IN LITIGATION OR ADMINISTRATIVE PROCEEDINGS

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

XV. AMENDMENT OF AGREEMENT

The County of Orange and the Contractor acknowledge that federal and state laws relating to data security and privacy are rapidly evolving and that amendment of this Agreement may be required to ensure compliance with such changes. Upon request by the County of Orange, the Contractor agrees to promptly enter into negotiations with the County of Orange concerning an amendment to this Agreement as may be needed by changes in federal and state laws and regulations or NIST 800-53. In addition to any other lawful remedy, the County of Orange may terminate this Agreement upon 30 days written notice if the Contractor does not promptly agree to enter into negotiations to amend this Agreement when requested to do so or does not enter into an amendment that the County of Orange deems necessary.

XVI. TERMINATION

This Agreement shall terminate on September 1, 2028, regardless of the date the Agreement is executed by the parties. The parties can agree in writing to extend the term of the Agreement. Contractor's requests for an extension shall be approved by the County of Orange and limited to no more than a six (6) month extension.

- A. **Survival:** All provisions of this Agreement that provide restrictions on disclosures of PII and that provide administrative, technical, and physical safeguards for the PII in the Contractor's possession shall continue in effect beyond the termination or expiration of this Agreement and shall continue until the PII is destroyed or returned to the County of Orange.

XVII. TERMINATION FOR CAUSE

Upon the County of Orange's knowledge of a material breach or violation of this Agreement by the Contractor, the County of Orange may provide an opportunity for the Contractor to cure the breach or end the violation and may terminate this Agreement if the Contractor does not cure the breach or end the violation within the time specified by the County of Orange. This Agreement may be terminated immediately by the County of Orange if the Contractor has breached a material term and the County of Orange determines, in its sole discretion, that cure is not possible or available under the circumstances. Upon termination of this Agreement, the Contractor shall return or destroy all PII in accordance with Section VII, above. The provisions of this Agreement governing the privacy and security of the PII shall remain in effect until all PII is returned or destroyed and the County of Orange receives a certificate of destruction.