

**Contract MA-063-26010204**  
**For**  
**Family Finding and Engagement Services**  
**Between**  
**Social Services Agency**  
**And**  
**Seneca Family of Agencies**



**CONTRACT**

**MA-063-26010204  
BETWEEN  
COUNTY OF ORANGE  
AND  
SENECA FAMILY OF AGENCIES  
FOR THE PROVISION OF  
FAMILY FINDING AND ENGAGEMENT SERVICES**

This Contract is by and between the County of Orange, hereinafter referred to as “County,” and Seneca Family of Agencies, a California non-profit corporation, 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 – OCSSA State Privacy and Security Provisions

**RECITALS**

WHEREAS, County issued a Request For Proposal for family finding and engagement services in 2025;

WHEREAS, County desires to contract with Contractor for the provision of family finding and engagement services;

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 Institution Code; and

ACCORDINGLY, THE PARTIES AGREED AS FOLLOWS:

## TERMS AND CONDITIONS

### 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 Termination Provisions 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.

### 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 Seneca Family of Agencies, for the Provision of Family Finding and Engagement Services, 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 and its personnel, described in the Personnel Disclosure paragraph of this Contract, who are subject to individual registration and/or licensing requirements, have all necessary licenses and permits required by the laws of the United States, State of California (hereinafter referred to as "State"), County of Orange, and all other appropriate governmental agencies to perform the services described in this Contract, and agrees to maintain, and require its personnel to maintain, these licenses and permits in effect for the duration of this Contract. Further, Contractor warrants that its employees shall conduct themselves in compliance with such laws and licensure requirements, including, without limitation, compliance with laws applicable to sexual harassment and ethical behavior. Contractor must notify 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. 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.
- E. Contractor shall cooperate with the California Department of Social Services (CDSS) on the implementation, monitoring, and evaluation of the State's Child Abuse and Neglect Prevention and

Intervention Program, and shall comply, to the mutual satisfaction of County and CDSS, with any and all reporting and evaluation requirements established by CDSS.

## **6. DELEGATION AND ASSIGNMENT/CHANGE OF OWNERSHIP**

### **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% 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. 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 7<sup>th</sup> 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]

**10. 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

*County of Orange  
Social Services Agency*

*MA-063-26010204  
Family Finding and Engagement Services*

*Page 8 of 120*

**CONTRACTOR:**

Seneca Family of Agencies  
8945 Golf Links Road  
Oakland, CA 94605

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.

**11. NOTICE OF DELAYS**

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

**12. 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.

**13. 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 \$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 Sexual Misconduct 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	\$1,000,000 combined single limit each accident
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 or per occurrence
Sexual Misconduct Liability	\$1,000,000 per occurrence or per claims-made

**14. 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.

**15. 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% 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.

**16. ANTI-PROSELYTISM PROVISION**

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

**17. SUPPLANTING GOVERNMENT FUNDS**

Contractor shall not supplant any federal, State, or County funds intended for the purposes of this Contract with any funds made available under this Contract. Contractor shall not claim reimbursement from County for, or apply sums received from County with respect to, that portion of its obligations which have been paid by another source of revenue. Contractor agrees that it shall not use funds received pursuant to this Contract, either directly or indirectly, as a contribution or compensation for purposes of obtaining federal, State, or County funds under any federal, State, or County program without prior written approval of County.

**18. EQUIPMENT**

- A. All items purchased with funds provided under this Contract, or which are furnished to Contractor by County, which have a single unit cost of at least \$10,000, including sales tax, shall be considered Capital Equipment. Title to all Capital Equipment shall, upon purchase, vest and remain in County. The use of such items of Capital Equipment is limited to the performance of this Contract. Upon the termination of this Contract, Contractor shall immediately return any items of Capital Equipment to County or its representatives, or dispose of them in accordance with the directions of County. Contractor further agrees to the following:
1. To maintain all items of Capital Equipment in good working order and condition, normal wear and tear excepted.
  2. To label all items of Capital Equipment, do periodic inventories as required by County, and to maintain an inventory list showing where and how the Capital Equipment is being used, in accordance with procedures developed by County. All such lists shall be submitted to County within 10 days of any request.
  3. To report in writing to County immediately after discovery, the loss or theft of any items of Capital Equipment. For stolen items, the local law enforcement agency must be contacted and a copy of the police report submitted to County.
  4. To purchase a policy or policies of insurance covering loss or damage to any and all Capital Equipment purchased under this Contract, in the amount of the full replacement value thereof, providing protection against the classification of fire, extended coverage, vandalism, malicious mischief, and special extended perils (all risks) covering the parties' interests as they appear.
- B. The purchase of any Capital Equipment by Contractor shall be requested in writing, shall require the prior written approval of County, and shall fulfill the provisions of this Contract which are appropriate and directly related to Contractor's service or activity under the terms of this Contract. County may refuse reimbursement for any costs resulting from Capital Equipment

purchased which are incurred by Contractor, if prior written approval has not been obtained from County.

- C. Computer Equipment - No computers and/or personal electronic devices, such as tablets and laptop computers, or any component thereof, may be purchased with funds provided under this Contract, regardless of purchase price, without prior written approval of County. Any such purchase shall be in accordance with specifications provided by County, be subject to the same inventory control conditions specified above in Subparagraphs 18.A.1 to 18.A.4, and, at the sole discretion of County, become the property of County upon termination of this Contract.

**19. 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 19.A.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.

**20. PAYMENTS**

- A. Maximum Contractual Funding Obligation
 

The maximum funding obligation of County under this Contract shall not exceed the amount of \$1,125,000 or actual allowable costs, whichever is less. The estimated annual amount for each 12 month period is as follows:

  - 1. \$375,000 for July 1, 2026, through June 30, 2027;
  - 2. \$375,000 for July 1, 2027, through June 30, 2028; and
  - 3. \$375,000 for July 1, 2028, through June 30, 2029.
- B. Allowable Costs
 

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

### C. Claims

1. Contractor shall submit monthly claims to be received by County no later than the twentieth (20th) calendar day of the month for expenses incurred in the preceding month, except as detailed below in Subparagraph 20.C.4. In the event the 20th calendar day falls on a weekend or County holiday, Contractor shall submit the claim the next business day. County holidays include New Year's Day, Martin Luther King Jr. Day, President Lincoln's Birthday, Presidents' Day, Memorial Day, Independence Day, Labor Day, Native American Day, Veterans Day, Thanksgiving Day, Friday after Thanksgiving Day, and Christmas Day.
2. All claims must be submitted on a form approved by County. County may require Contractor to submit supporting source documents with the monthly claim, including, inter alia, a monthly statement of services, general ledgers, supporting journals, time sheets, invoices, canceled checks, receipts, and receiving records, some of which may be required to be copied. Source documents that Contractor must submit shall be determined by County and/or County's Auditor-Controller. Contractor shall retain all financial records in accordance with Paragraph 25 of this Contract.
3. Payments should be released by County within a reasonable time period of approximately 30 days after receipt of a correctly completed claim form and required supporting documentation.
4. Year-End and Final Claims
  - a. Contractor shall submit a final claim for each County fiscal year, July 1 through June 30, covered under the term of this Contract, as stated in Paragraph 1, by no later than August 30th of each corresponding County fiscal year. Claims received after August 30th of each corresponding County fiscal year may, at County's sole discretion, not be reimbursed. County may modify the date upon which the final claim per each County fiscal year must be received, upon written notice to Contractor.
  - b. The basis for final settlement shall be the actual allowable costs as defined in Title 45 CFR and 2 CFR, Part 200, incurred and paid by Contractor pursuant to this Contract; limited, however, to the maximum funding obligation of County. In the event that any overpayment has been made, County may offset the amount of the overpayment against the final payment. In the event overpayment exceeds the final payment, Contractor shall pay County all such sums within five business days of notice from County. Nothing herein shall be construed as limiting the remedies of County in the event an overpayment has been made.

## 21. OVERPAYMENTS

Any payment(s) made by County to Contractor in excess of that to which Contractor is entitled under this Contract shall be repaid to County, in accordance with any applicable regulations and/or policies in effect during the term of this Contract, or as established by County procedure. Any overpayments made by County which result from a payment by any other funding source shall be repaid, at the discretion of County, to 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 County by the funding source, then Contractor shall reimburse County within 30 days thereafter and prior to any administrative appeal process. Contractor agrees to pay all costs incurred by County necessary to enforce the provisions set forth in this Paragraph.

**22. OUTSTANDING DEBT**

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

**23. 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.

**24. 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.

**25. 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.

**26. 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](http://www.nsopw.gov)) and Megan's Law Sex Offender Registry ([www.meganslaw.ca.gov](http://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 26.D and 26.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 26.D and 26.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.

## **27. EMPLOYMENT ELIGIBILITY VERIFICATION**

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

**28. CHILD AND DEPENDENT ADULT/ELDER ABUSE REPORTING**

Contractor shall establish a procedure acceptable to 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

**29. NOTICE TO EMPLOYEES REGARDING THE SAFELY SURRENDERED BABY LAW**

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

**30. 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, case law, 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 child to be interviewed, photographed, or recorded by any publication or organization, or to appear on any radio, television, or internet broadcast or make any other public appearance. Such approval shall be requested through child's Social Worker.

**31. SECURITY**

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

**32. COPYRIGHT ACCESS**

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

**33. WAIVER**

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

**34. SERVICES DURING EMERGENCY AND/OR DISASTER**

- 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. With the exception of

overtime hours which require pre-authorization, reimbursement of ordinary expenditures provided during or after an emergency/disaster shall be calculated by the same rates that apply during non-emergency/disaster conditions. Additionally, any costs to continue services to clients during an emergency and/or disaster shall be incurred by the Contractor. These costs may include, but are not limited to: Personal Protective Equipment or other supplies necessary to conduct business during an emergency and/or disaster.

- 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.

**35. 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; 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
  3. 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://cio.ocgov.com/egovernment-policies>.

**36. 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.

**37. ENERGY EFFICIENCY STANDARDS**

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

**38. ENVIRONMENTAL PROTECTION STANDARDS**

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

- 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.

**39. 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

#### **40. POLITICAL ACTIVITY**

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

#### **41. TERMINATION PROVISIONS**

- 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.

#### **42. COOPERATIVE CONTRACT**

- A. This Contract is a cooperative contract and may be utilized by all County of Orange departments.
- B. The provisions and pricing of this Contract may be extended, at the option of Contractor, to any Municipal, County, Public Utility, Hospital, Educational Institution, or any other non-profit or governmental organization (the "Cooperative Program"). Parties in a Cooperative Program wishing to use this Contract will be responsible for issuing their own purchase documents / price agreements, providing for their own acceptance, and making any subsequent payments. Contractor shall be required to include in any agreement entered into with another agency or entity that is entered into pursuant to the provisions and pricing of this Contract a clause that binds the parties to the agreement to "indemnify, defend with counsel approved in writing by the County of Orange, California ("County"), and hold County, its elected and appointed officials, officers, employees, agents and those special districts and agencies which County's Board of Supervisors acts as the governing Board ("County Indemnitees") harmless from any claims, demands or liability of any kind or nature, including but not limited to personal injury or property damage, arising from or related to the services, products or other performance provided" under the agreement. Failure to so include this clause voids the Contract's extension to a Cooperative Program and will be considered a material breach of this Contract and grounds for immediate Contract termination. The cooperative entities are responsible for obtaining all certificates of insurance and bonds required. The County of Orange makes no guarantee of usage by other users of this Contract.
- C. Subordinate contracts must be executed prior to the expiration or earlier termination of this Contract and may survive the expiration of this Contract. This Cooperative Contract provision shall survive expiration or termination of this Contract.

#### **43. GOVERNING LAW AND VENUE**

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

**44. SIGNATURE IN COUNTERPARTS**

- 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**

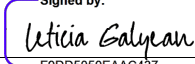
IN WITNESS WHEREOF, the Parties hereto have executed this Contract the date set forth opposite their signatures.

If Contractor is a corporation, Contractor shall provide two signatures as follows:

- 1) the first signature must be either the Chairman of the Board, the President, or any Vice President;
- 2) the second signature must be that of the Secretary, an Assistant Secretary, the Chief Financial Officer, or any Assistant Treasurer.

In the alternative, a single corporate signature is acceptable when accompanied by a corporate resolution or by-laws demonstrating the legal authority of the signature to bind the company.

**Contractor:** Seneca Family of Agencies

 <small>Signed by: F9DD5060EAAAC437...</small> Signature	Leticia Galyean	CEO	3/27/2026   9:16:22 AM PDT
	Name	Title	Date

Signature	Name	Title	Date
-----------	------	-------	------

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

**COUNTY AUTHORIZED SIGNATURE:**

Signature	Name	Deputy Procurement Agent	Date
-----------	------	--------------------------	------

Approved as to form:

**County Counsel**

 <small>DocuSigned by: DAA59997690B425...</small> Signature	Carolyn Frost	<b>Deputy</b>	3/27/2026   1:34:37 PM PDT
	Name	Title	Date

**ATTACHMENT A - SCOPE OF WORK****1. POPULATION TO BE SERVED**

Contractor shall provide FFES to find and engage family members and/or other supportive adults with children, youth, and young adults in foster care who have non-existent or distant connections with family members or other supportive adults and who could be experiencing complex care needs as referred by County as defined below:

- A. Children/youth are defined as individuals up to 18 years of age, who are dependents of the Orange County Juvenile Court, and placed in out-of-home care; and
- B. Young adults are defined as individuals who are 18 to 21 years of age, who are dependents of the Orange County Juvenile Court, and placed in out-of-home care.

The children/youth/young adults to be served shall be hereinafter referred to as “Client/Clients.”

**2. DEFINITIONS**

- A. Children and Family Services (CFS): The division in the Social Services Agency (SSA) that provides services to protect children from abuse and neglect, and at-risk Families.
- B. Child Family Team (CFT) meetings: A meeting of a group of individuals convened by SSA, who are engaged through a variety of team-based processes to identify the strengths and needs of the child/youth and his or her family to help achieve positive outcomes for safety, permanency, and well-being.
- C. Family Finding and Engagement Services (FFES): A collection of strategies that help locate and engage family members and fictive kin (also known as a nonrelative extended family member, or NREFM) for children who enter foster care, aim to find relatives and other important adults who can provide permanent homes for children and youth, or caring, lifelong support networks that can provide relational permanence if relatives are unable to care for children in their homes.
- D. Fictive Kin: A nonrelative extended family member, which is defined as an adult caregiver who has an established familial relationship with a relative of the child or a familial or mentoring relationship with the child.
- E. Relational Permanency: Lifelong connections to caring adults, including at least one adult who will provide a permanent, parent-like connection for that youth.
- F. Youth: A dependent or ward of the Orange County Juvenile Court, birth through age 21, who is placed in out-of-home care and a party to the referral made for FFES

### 3. **GOALS, STRATEGIES, AND OUTCOME OBJECTIVES**

A. The primary goals of FFES are to:

1. Increase family connections for Clients in care;
2. Increase connections and placements with relatives and NREFM when Clients first enter out-of-home care, and to increase legal and relational permanency for Clients who have been in out-of-home care for a longer time;
3. Increase the success of identifying and engaging relatives and other supportive adults to support Clients during and after reunification, and support permanency in cases where reunification cannot occur; and
4. Reduce the length of stay in foster care.

B. The outcome objectives are as follows:

1. For at least 90% of referrals, at least three identified connections are located, contacted, and have initiated engagement with the youth/young adult (e.g., exchanged emails or phone calls) within 60 days of referral.
2. At least 75% of youth referred will attend at least two-family or supportive adult engagement meetings, visitations, or activities within the first 90 days of referral.
3. At least 75% of youth will report an increased sense of belonging and connectedness to supportive adults, measured via the Youth Connections Scale, which may be modified if deemed appropriate by the County.
4. Any barriers that impact progress toward outcome objectives will be discussed during monthly county meetings and reports.

C. For the purposes of measuring and attaining outcomes and goals, Contractor shall implement the following in providing FFES services:

1. Contractor must complete the following steps to initiate connection within 30 days of receipt of any referral:
  - a) Receive, date stamp, and provide initial review of all referrals sent by SSA.
  - b) Contact a social worker associated to the case to acknowledge receipt of the referral and to coordinate initiation of services.
  - c) Create a case file unique to each Client, ensuring that those who are part of a sibling set can be easily identified. Each sibling should have a separate case file.
  - d) Initiate comprehensive family finding and engagement strategies and techniques to achieve the goals referenced in this scope of work.

2. Contractor shall integrate client surveys into the FFES program.
  - a) Contractor shall administer a survey utilizing the Youth Connections Scale during the termination of the referral.
  - b) Contractor shall submit surveys to County within 15 calendar days of service termination and /or upon request of County.
  - c) County shall retain the right to change the survey and survey methodology during the contract term.

#### 4. **WORKLOAD STANDARDS**

- A. Contractor agrees to the following:
  1. Siblings referred [two or more Clients] will be counted as one Client, if they have the same parents.
- B. Contractor's workload standards with respect to this Scope of Work are as follows:
  1. Provide FFES for up to 60 Clients referred by County for each fiscal year of the term of this Contract.
  2. With concurrence of County, close referral once new family members/supportive adults have been engaged and there is a stable plan to sustain relationship with Client. If County deems appropriate, County may unilaterally close a referral.
  3. Contractor and County may mutually agree in writing to modify workload standards as set forth in this Paragraph and as authorized by County, without reducing the level of service to be provided by Contractor.

#### 5. **HOURS OF OPERATION**

- A. Contractor shall provide services during hours that are responsive to the needs of the population(s) to be served as determined by County. At a minimum, Contractor shall provide services Monday through Friday, from 8:00 a.m. to 5:00 p.m., except County holidays as established by the Orange County Board of Supervisors. However, Contractor is encouraged to provide the contracted services on holidays, whenever possible.
- B. Contractor's holiday schedule shall not exceed County's holiday schedule which is as follows: New Year's Day, Martin Luther King Jr. Day, President Lincoln's Birthday, Presidents' Day, Memorial Day, Independence Day, Labor Day, Native American Day, Veterans Day, Thanksgiving Day, Friday after Thanksgiving Day and Christmas Day. Contractor shall obtain prior written approval from County for any closure outside

of County's holiday schedule and the hours listed in this Scope of Work. Any unauthorized closure shall be deemed a material breach of this Contract and shall not be reimbursed.

**6. SERVICES TO BE PROVIDED**

Contractor shall provide the following services:

- A. Contractor shall establish or re-establish a relationship between Client and one or more adults with a known connection. Services to include, but not limited to, review of case files; interviews with Client and family members/other supportive adults; telephone calls; internet searches; e-mail communications; in-person visits; engagement strategies; and individualized FFES plans will be designed to increase the rate of family reunification, kinship placements, and overall connections for Clients while in care.
- B. Contractor shall implement family-centered, family-friendly, collaborative, linguistically, and culturally responsive services.
- C. Contractor shall implement family finding and engagement practices through a trauma informed lens, as described by the National Child Traumatic Stress Network (<https://www.nctsn.org/>).
- D. Contractor shall maintain regular communication with County and each Client's social worker, at least monthly, throughout the period of search for family members/supportive adults and engagement activities with those family members/supportive adults.
- E. Contractor shall collaborate with Client's social worker to identify other resources or services to support Client's positive reunification and/or relational permanency outcomes.
- F. Contractor shall attend meetings, as requested by County, as they relate to FFES.
- G. Contractor shall deliver services in the home of the Client, homes of family members and other supportive adults, or at other mutually agreed upon sites including virtually through interactive video conferencing technology and phone calls.
- H. 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 family members and/or other supportive adults who will have direct, interactive contact with Clients served through this Agreement: U.S. Department of Justice National Sex Offender Website ([www.nsopw.gov](http://www.nsopw.gov)), Megan's Law Sex Offender Registry ([www.meganslaw.ca.gov](http://www.meganslaw.ca.gov)) (or equivalent in other state), and County Superior Court Criminal and Traffic Case system in which the individual resides (e.g., Orange County Superior Court of California Criminal and Traffic Cases - <http://www.occourts.org/>).

- I. Contractor shall obtain appropriate consent to contact Client's therapist to consult on the best approach to initiate meeting new family members/supportive adults, and conduct consultation with the therapist.
- J. Contractor shall deliver FFES in Orange County, other California counties, other states throughout the country, and other countries as needed, to find and engage family members and other supportive adults related to the Client.
- K. Contractor and County may mutually agree in writing to modify services to be provided as set forth in this Paragraph and as authorized by County, without reducing the level of service to be provided by Contractor.

## 7. **FACILITIES**

Administrative services under this Contract shall be provided at:

Seneca Family of Agencies  
 233 S Quintana Drive  
 Anaheim, CA 92807

Contractor's facilities shall be safe, clean, and maintained in compliance with all applicable laws, rules, regulations, building codes, statutes, and orders, as they now exist or may be subsequently amended.

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

## 8. **REPORTING REQUIREMENTS**

Contractor shall prepare and submit to County written reports, including, but not limited to:

- A. Monthly Aggregate Outcomes and Statistical Report
  - 1. Contractor shall prepare and submit to County a monthly outcomes report, in a format approved by the County, by the 10th calendar day of the month for the preceding month's services.
  - 2. The report will include, but not be limited to, a listing of the names of all active cases; the number of referrals received; the number of new cases opened; the number of active cases, in each stage of the FFES process, on the last day of the month; the number of cases closed; a breakdown by age group to delineate Clients; the number of Clients for whom connections were established in that month; the average length of time invested to achieve connections; progress regarding outcome objectives; and other information as requested by County.

#### B. Individual Client Status Report

1. Contractor shall prepare and submit a monthly status report to each Client's assigned social worker, in a format approved by County, by the 10th calendar day of the month for the preceding month's services.
2. The report will include, but not be limited to, a summary that documents Contractor's diligence in responding to the referral, as well as the outcomes achieved.
3. The summary will include a list of all family members and/or other supportive adults identified, located and/or contacted. This listing will be in a written and/or visual format, and will include the relationship and engagement status of each of the contacts/connections.
4. The report will include plans for FFES to be provided in the following month.

#### C. Youth Informed Connections Plan

1. Participating youth will have a written, youth-informed Connections Plan within 180 days of referral, identifying at least three adults committed to ongoing engagement support plan. If services cease for a client within 180 days of referral, the Connections Plan will not be required to be submitted, but the final report must still be submitted and include all available information that would have otherwise been in the Connections Plan.
2. This report shall be submitted on a form that is approved by County. County may revise the form at their sole discretion.

#### D. Intensive Relative Search and Engagement Final Report

1. Upon closure of services for each Client, Contractor shall prepare and submit a final report which will include, but not be limited to:
  - a. A written summary of all information gleaned from County's case files, additionally secured records, and interviews with Client, Client's social worker, and Client's family members/supportive adults, etc.
  - b. Date of entry into FFES and date of exit from FFES.
  - c. A visualization of the known and discovered connections (e.g., family tree, etc.) in a format approved by County.
  - d. A service exit plan to sustain and grow the connections upon termination of FFES.

**9. UTILIZATION REVIEW**

- A. Contractor and County’s designee shall meet at least annually to review and evaluate a random selection of family case records. The review may include, but is not limited to, an evaluation of the necessity and appropriateness of services provided and length of services. Family 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 Children and Family Services 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 Children and Family Services for final resolution. Nothing in this subparagraph shall affect County’s termination rights under the Termination clauses of this Contract.

**10. BUDGET**

The annual budget for services provided pursuant to the Scope of Work of this Contract is set forth as follows:

**Budget for July 1, 2026 through June 30, 2027**

Salaries and Benefits	Position Type <sup>(1)</sup>	FTEs <sup>(2)</sup>	Maximum Hourly Rate <sup>(3)</sup>	Amount
Program Supervisor	D	0.85	\$56.33	
Family Finder	D	2.00	\$35.83	
Regional Executive Director	A	0.02	\$101.96	
Senior Administrative Assistant	A	0.02	\$39.00	
Quality Assurance Manager	A	0.02	\$60.84	
Program Assistant/Quality Assurance Specialist	A	0.20	\$39.00	
Financial Analyst	A	0.01	\$61.40	
Facilities Manager	A	0.03	\$65.03	
Supplemental Overtime/Stipends/Bonuses Pool				
<b>Total Salaries</b>				<b>\$219,114</b>

Benefits <sup>(4)</sup>	<u>\$59,161</u>
Total Salaries & Benefits	\$278,275
Services and Supplies <sup>(6)</sup>	\$31,041
Operating Expenses <sup>(7)</sup>	<u>\$16,771</u>
Total Salaries, Benefits & Operating Expenses	\$326,087
Indirect Costs (15%) <sup>(5)</sup>	<u>\$48,913</u>
Total Annual Maximum Obligation <sup>(8)</sup>	\$375,000

**Budget for July 1, 2027 through June 30, 2028**

Salaries and Benefits	Position Type <sup>(1)</sup>	FTEs <sup>(2)</sup>	Maximum Hourly Rate <sup>(3)</sup>	Amount
Program Supervisor	D	0.72	\$56.33	
Family Finder	D	2.00	\$35.83	
Regional Executive Director	A	0.02	\$101.96	
Senior Administrative Assistant	A	0.02	\$39.00	
Quality Assurance Manager	A	0.02	\$60.84	
Program Assistant/Quality Assurance Specialist	A	0.20	\$39.00	
Financial Analyst	A	0.01	\$61.40	
Facilities Manager	A	0.03	\$65.03	
Supplemental Overtime/Stipends/Bonuses Pool				
Total Salaries				\$219,114
Benefits <sup>(4)</sup>				<u>\$59,161</u>
Total Salaries & Benefits				\$278,275
Services and Supplies <sup>(6)</sup>				\$31,041
Operating Expenses <sup>(7)</sup>				<u>\$16,771</u>
Total Salaries, Benefits & Operating Expenses				\$326,087
Indirect Costs (15%) <sup>(5)</sup>				<u>\$48,913</u>
Total Annual Maximum Obligation <sup>(8)</sup>				\$375,000

**Budget for July 1, 2028 through June 30, 2029**

Salaries and Benefits	Position Type <sup>(1)</sup>	FTEs <sup>(2)</sup>	Maximum Hourly Rate <sup>(3)</sup>	Amount
Program Supervisor	D	0.60	\$56.33	
Family Finder	D	2.00	\$35.83	
Regional Executive Director	A	0.02	\$101.96	
Senior Administrative Assistant	A	0.02	\$39.00	
Quality Assurance Manager	A	0.02	\$60.84	
Program Assistant/Quality Assurance Specialist	A	0.20	\$39.00	
Financial Analyst	A	0.01	\$61.40	
Facilities Manager	A	0.03	\$65.03	
Supplemental Overtime/Stipends/Bonuses Pool				
Total Salaries				\$219,114
Benefits <sup>(4)</sup>				<u>\$59,161</u>
Total Salaries & Benefits				\$278,275
Services and Supplies <sup>(6)</sup>				\$31,041
Operating Expenses <sup>(7)</sup>				<u>\$16,771</u>
Total Salaries, Benefits & Operating Expenses				\$326,087
Indirect Costs (15%) <sup>(5)</sup>				<u>\$48,913</u>
Total Annual Maximum Obligation <sup>(8)</sup>				\$375,000

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

(2) For hourly employees, Full-Time Equivalent (FTE) is defined as the amount of time (stated as a percentage) the position will be providing services under the terms of this Contract. This

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

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

(4) Employee Benefits include FICA, Unemployment, Worker's Compensation, paid time off, pension, medical insurance, dental insurance, vision insurance, life insurance, identity theft protection, fingerprinting costs, and expense for accrued vacation time payout, for a separated employee, limited to the actual vacation time accrued during the fiscal year in which the expense is claimed, minus the actual vacation time used by the employee during said fiscal year. The overall benefit rate shall not exceed 27% of the actual salary expense claimed.

(5) Indirect cost includes administrative cost not directly charged to the program including agency executive leadership, centralized agency departments that do not work directly in program, and other non-payroll costs. Indirect costs are based on 15% of salaries and benefits, services and supplies, and operating expenses. In the event the indirect cost rate is reduced, the reduction shall be afforded to County and the budget amended accordingly. Contractor shall provide notification to County of any changes in the rate.

(6) Services and supplies shall include family finding search services, permanency consultation, program supplies and subscriptions, telephone, staff training and professional development, travel and mileage reimbursement, staff recruitment, general insurance, and treatment supplies. Mileage is limited to the amount allowed by IRS. Treatment supplies include items that support a youth with engagement in services or engagement in the connection/engagement process, which may include fidget tools or coping items to help youth manage emotions during visits with connections, art supplies to create cards/artwork during engagement processes, and games to support with rapport building or encourage interactions with identified connections.

(7) Operating expenses shall include government taxes, building maintenance and supplies, utilities, expendable equipment, equipment expense, vehicle operating, and facility expenses.

(8) The annual budgets are estimated and subject to modification per this Scope of Work, providing that such modifications do not change the County's maximum funding obligation as stated in the "Payments" Paragraph of this Contract.

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

Contractor and County may agree, subject to advance written notice, to add, delete or modify line items and/or amounts and/or the number and type of FTE positions without changing County's maximum funding obligation as stated in the "Payments" Paragraph of this Contract or reducing the level of service to be provided by Contractor. Further, in accordance with the

Termination provisions of this Contract, in the event County reduces the maximum funding obligation as stated in the "Payments" Paragraph, Contractor and County may mutually agree in writing to proportionately reduce the service goals as set forth in this Attachment. Failure to obtain advance written approval for any proposed Budget Modification Request may result in disallowance of reimbursement for those costs.

In the event one of the annual budgets shown in the Scope of Work of this Contract is modified, the modification shall remain in effect until the end of the specific fiscal period modified. For example, if the annual budget for the term of July 1, 2026 through June 30, 2027 is modified, the modification will be effective until June 30, 2027. Beginning July 1, 2027, the budget will revert to the budget included in the Scope of Work of this Contract until it is modified, if applicable.

## 11. **STAFFING REQUIREMENTS**

- A. Contractor shall be responsible for providing training and maintaining a competent, stable, and experienced workforce to fulfill service requirements. Contractor's staff shall be able to read, write, speak, and understand English. If Client/Family contact is required to obtain the required documentation or provide services, Contractor will be required to provide translation services for languages needed so that all Client(s)/Families are provided services in their primary language.
- B. Contractor shall use a formal recruitment plan which complies with federal and State employment and labor regulations. Contractor shall recruit and maintain trained personnel who are responsive to, and who understand, the diversity of cultures which can be found among the client population identified in the Scope of Work. Contractor shall employ staff with the background, training, and experience to provide contracted services.
- C. Contractor shall provide the following described staff positions during the entire term of the Contract:

### 1. Regional Executive Director

#### Duties:

- a. Oversees and administers program, including ensuring the delivery of high-quality services and providing program continuity;
- b. Plan for future program growth and development; and
- c. Conducts regular meetings to ensure fiscal accountability and alignment with County Contract strategic objectives.

Qualifications:

- a. Master's degree in psychology, social work, human behavior or a related field from an accredited school and licensed as a Licensed Marriage and Family Therapist (LMFT) or Licensed Clinical Social Worker (LCSW);
- b. At least three years' experience in the development of new programs within the mental health field;
- c. Master's degree in social work or related field (license preferred);
- d. Strong writing and communication skills;
- e. Supervisory experience; and
- f. Valid driver's license.

2. Program Supervisor

Duties:

- a. Receives, prioritizes, and assigns referrals, and provides supervision for Family Finding direct service staff, coordinates and supports communication with the County, and ensures timely and regular reporting to the County; and
- b. Provides direct support to supervisees, oversees the quality and tracking of all services and documentation, trains and onboards new staff, ensures program coverage which may include carrying a family finder caseload with the duties it entails, and provides management.

Qualifications:

- a. Master's degree in social work or related field, or bachelor's degree with three years of experience providing direct services;
- b. Ability to work as part of and supervise a multidisciplinary team;
- c. Experience working with children in out of home care preferred;
- d. Experience implementing family-focused services preferred;
- e. Ability to work with a diverse population;
- f. Willingness to respond to crisis situations (as needed);
- g. Valid driver's license; and
- h. Minimum of two years of supervisory experience with the treatment of children and families, preferably in the area of child sexual abuse.

3. Family Finder

Duties:

- a. Provides assessment and counseling for complex cases;
- b. Searches for family members, fictive kin or natural supports of youth under the age of 21 referred by the County;
- c. Works closely with a youth's Social Worker and Child and Family Team to identify connections the youth has lost contact with due to placement in foster care;
- d. Conducting thorough case record reviews and family finding members and other meaningful people who can provide positive support and a permanent lifelong connection to the youth being served;
- e. Work closely with the SSA social worker and other providers to prepare and support the youth for initial and ongoing contact; and
- f. Documenting the findings and progress made for each case in reports that are shared with each youth's social worker.

Qualifications:

- a. Bachelor's degree in a related field, or associate's degree and one year of applicable experience, or a high school diploma and two years of applicable work or lived experience;
- b. Must show a combination of experience and demonstrated interest in helping youth maintain or gain contact with relatives;
- c. Demonstrated competence in the skill areas of positive client engagement and communication;
- d. Must have experience working with system involved youth and demonstrated understanding of the issues they potentially face;
- e. Good writing skills for documentation; and
- f. Valid California's driver license.

4. Senior Administrative Assistant

Duties:

- a. Assist the Regional Executive Director and other members of the leadership team in matters of communication and organization as pertaining to this Contract.

Qualifications:

- a. Bachelor's degree and one year of experience, or associate's degree and two years of experience, or high school diploma/general education development (GED) certificate and three years of applicable work experience;
- b. Excellent organizational, analytical, writing, typing, editing, and formatting skills;
- c. Strong communication skills;
- d. Proficiency with Microsoft Office suite, Adobe suite, and electronic databases; and
- e. At least 21 years old and valid driver's license.

5. Quality Assurance Manager

Duties:

- a. Responsible for developing, implementing, and monitoring quality assurance processes to ensure compliance with regulatory standards, accreditation requirements, and organizational policies as pertaining to this Contract; and
- b. Supervises Program Assistants and/or Quality Assurance Specialists and collaborates with departmental and program leadership to promote a culture of excellence in service delivery for this Contract.

Qualifications:

- a. Bachelor's degree, or associate's degree or equivalent and two years of applicable work experience, or high school diploma/GED and three years of applicable work experience;
  - b. Excellent organizational, analytical, and communication skills;
  - c. Proficiency in Microsoft Word, Outlook, and Excel preferred;
  - d. Experience managing Electronic Health Records;
  - e. Ability to prioritize projects, manage deadlines, and problem-solve; and
  - f. At least 21 years old and valid driver's license.
6. Program Assistant/Quality Assurance Specialist

Duties:

- a. Responsible for ensuring compliance with regulatory standards, accreditation requirements, and organizational policies pertaining to this Contract; and
- b. Compiles, updates, and organizes all documentation for clients in collaboration with program staff, program leaders, and centralized administrative teams to ensure Contract compliance.

Qualifications:

- a. Bachelor’s degree, or associates degree and two years of applicable work experience, or high school diploma/GED and three years of applicable work experience;
  - b. Ability to compile and track documents according to strict guidelines and regulations;
  - c. Excellent organizational, problem solving, and time management skills;
  - d. Demonstrated proficiency in Microsoft Office suite, Zoom, Teams, and a variety of technology platforms;
  - e. Ability to structure and perform routine tasks; and
  - f. At least 21 years old and valid driver’s license.
7. Financial Analyst

Duties:

- a. Responsible for leading cross-functional workflows, collaboration, and communication between program leadership and centralized administrative departments to identify, develop, and monitor systems to improve Contractor’s ability to successfully meet its fiscal, contractual, and programmatic goals and obligations as pertaining to this Contract.

Qualifications:

- a. Bachelor’s in related field, or associate’s degree and one year of applicable work experience, or high school diploma and two years of applicable work experience;
- b. At least five years of professional work experience;
- c. Experience in program improvement, systems development, and/or organizational development preferred;
- d. Direct care or administrative experience in mental health, child welfare, juvenile justice and/or education systems strongly desired;
- e. Experience in, or demonstrated aptitude, for program operations, including budget development and/or fiscal management;
- f. Computer literacy with Microsoft Office Suite, including a high level of knowledge of Excel; and
- g. At least 21 years old and valid driver’s license.

8. Facility Manager

Duties:

- a. Responsible for all major construction and maintenance projects necessary for the safe running of Contractor as pertaining to this Contract;
- b. Main duties include supervising, managing the maintenance budget, and performing general maintenance and repair of agency properties and equipment pertaining to Contract;
- c. Maintains practical skill and knowledge in trades such as painting, carpentry, plumbing, masonry, and electrical work; and
- d. Maintains current knowledge of Joint Commission, Community Care Licensing, Cal- OSHA and all other applicable regulations and requirements.

Qualifications:

- a. Five years of general maintenance or related experience;
- b. At least two years of experience in managing a variety of maintenance and construction tasks;
- c. Two years supervisory experience;
- d. Strong organizational skills;
- e. High school diploma or equivalent informal education sufficient to ensure ability to perform job duties;
- f. Knowledge of maintaining facilities and grounds in a safe, clean, and orderly condition; and
- g. Solid knowledge of various computer programs.

12. **TRAINING**

- A. Contractor’s staff shall attend SSA trainings, conferences, and meetings as required by SSA.
- B. Contractor shall provide Contractor’s staff with onboarding, as well as ongoing trainings and assistance to ensure that service deliverables are met.
- C. Contractor shall ensure that Contractor’s staff receives cultural awareness and responsiveness training.

- D. Contractor shall maintain a log of in-house training activities for Contractor's staff. This log shall be made available to SSA, upon request.

**13. QUALITY ASSURANCE/QUALITY CONTROL**

Contractor shall utilize a comprehensive Quality Control Plan, on a format approved by SSA, to monitor the level of program service and quality. The Quality Control Plan shall be effective upon Contract start date and will be updated and resubmitted for SSA approval when changes occur. The Quality Control Plan will include, but not be limited to, the following:

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

**ATTACHMENT B - 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.oc.gov](mailto:Andrew.Alipanah@ocit.oc.gov)

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

**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 4 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. Passwords characters will not be repeated in a row (Do not use: P@\$\$\$ . This is ok: P@\$\$\$)
  - vii. COMPLEX PASSWORD EXAMPLE: P@\$\$WoRd13
  - 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.
- n. Contractor may implement equivalent safeguards described in NIST Special Publication 800-63B – Digital Identity Guidelines as an alternative to some of all the above password controls.

### **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, anti-spyware, personal firewall, host-based intrusion detection (IDS), network-based intrusion detection (IDS), intrusion prevention systems (IPS), and whitelisting and blacklisting of applications, web sites, and IP addresses.
2. 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****OCSSA 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. If applicable, 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 10 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)

<b>Control Number</b>	AC-1
<b>Title</b>	Access Control Policy and Procedures
<b>DHCS &amp; CDSS Requirement</b>	<p>The organization must:</p> <ul style="list-style-type: none"> <li>a. Develop, document, and disseminate to designated organization officials: <ul style="list-style-type: none"> <li>1. An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance;</li> <li>2. Procedures to facilitate the implementation of the access control policy and associated access control controls;</li> </ul> </li> <li>b. Review and update the current access control procedures with the organization-defined frequency.</li> </ul>
<b>Supplemental Guidance (from NIST 800-53)</b>	<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>
<b>Control Number</b>	AC-2
<b>Title</b>	Account Management
<b>DHCS &amp; CDSS Requirement</b>	<p>The organization must:</p> <ul style="list-style-type: none"> <li>a. Identify and select the accounts with access to PII to support organizational missions/business functions.</li> <li>b. Assign account managers for information system accounts;</li> <li>c. Establish conditions for group and role membership;</li> <li>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;</li> <li>e. Require approvals by designated access authority for requests to create information system accounts;</li> <li>f. Create, enable, modify, disable, and remove information system accounts in accordance with organization account management procedures;</li> <li>g. Monitors the use of information system accounts;</li> <li>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.</li> <li>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.</li> <li>j. Review accounts for compliance with account management requirements according to organization-based frequency; and</li> </ul>

	<p>k. Establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.</p>
<p><b>Supplemental Guidance (from NIST 800-53)</b></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><b>Control Number</b></p>	<p>AC-3</p>
<p><b>Title</b></p>	<p>Account Management</p>
<p><b>DHCS &amp; CDSS Requirement</b></p>	<p>The organization must:</p> <ul style="list-style-type: none"> <li>a. Identify and select the accounts with access to PII to support organizational missions/business functions.</li> <li>b. Assign account managers for information system accounts;</li> <li>c. Establish conditions for group and role membership;</li> <li>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;</li> <li>e. Require approvals by designated access authority for requests to create information system accounts;</li> <li>f. Create, enable, modify, disable, and remove information system accounts in accordance with organization account management procedures;</li> <li>g. Monitors the use of information system accounts;</li> <li>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.</li> <li>i. Authorizes access to the information systems that receive, process, store or transmit PII</li> </ul>

	<p>based on valid access authorization, need-to-know permission or under the authority to re-disclose PII.</p> <ul style="list-style-type: none"> <li>j. Review accounts for compliance with account management requirements according to organization-based frequency; and</li> <li>k. Establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.</li> </ul>
<p><b>Supplemental Guidance (from NIST 800-53)</b></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><b>Control Number</b></p>	<p>AC-3(7)</p>
<p><b>Title</b></p>	<p>Access Enforcement   Role-Based Access Control</p>
<p><b>DHCS &amp; CDSS Requirement</b></p>	<p>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.</p>
<p><b>Supplemental Guidance (from NIST 800-53)</b></p>	<p>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</p>

	by the policy.
<b>Control Number</b>	AC-3(8)
<b>Title</b>	Access Enforcement   Revocation of Access Authorization
<b>DHCS &amp; CDSS Requirement</b>	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.
<b>Supplemental Guidance (from NIST 800-53)</b>	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.
<b>Control Number</b>	AC-4
<b>Title</b>	Information Flow Enforcement
<b>DHCS &amp; CDSS Requirement</b>	The organization information system must: enforce approved authorizations for controlling the flow of information within the system and between interconnected systems based on the need for interconnected systems to share PII to conduct business.
<b>Supplemental Guidance (from NIST 800-53)</b>	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. 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. 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. 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. 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
<b>Control Number</b>	AC-5
<b>Title</b>	Separation of Duties
<b>DHCS &amp; CDSS Requirement</b>	<p>The organization must:</p> <ul style="list-style-type: none"> <li>a. Separate organization-defined duties of individuals;</li> <li>b. Document separation of duties of individuals; and</li> <li>c. Defines information system access authorizations to support separation of duties.</li> </ul> <p><i>DHCS and CDSS also require that the state organization prohibit any functional 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>
<b>Supplemental Guidance (from NIST 800-53)</b>	<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> <ul style="list-style-type: none"> <li>(i) dividing mission functions and information system support functions among different individuals and/or roles;</li> <li>(ii) conducting information system support functions with different individuals (e.g., system management, programming, configuration management, quality assurance and testing, and network security); and</li> <li>(iii) ensuring security personnel administering access control functions do not also administer audit functions.</li> </ul> <p>Related controls: AC-3, AC-6, PE-3, PE-4, PS-2.</p>
<b>Control Number</b>	AC-6
<b>Title</b>	Least Privilege
<b>DHCS &amp; CDSS Requirement</b>	<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>
<b>Supplemental Guidance (from NIST 800-53)</b>	<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.</p> <p>Related controls: AC-2, AC-3, AC-5, CM-6, CM-7, PL-2.</p>
<b>Control Number</b>	AC-6(1)
<b>Title</b>	Least Privilege   Authorize Access to Security Functions
<b>DHCS &amp; CDSS Requirement</b>	<p>The organization must explicitly authorize access to organization-defined security functions (deployed in hardware, software, and firmware) and security-relevant information.</p>
<b>Supplemental Guidance (from NIST 800-53)</b>	<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>
<b>Control Number</b>	AC-6(7)

<b>Title</b>	Least Privilege   Review Of User Privileges
<b>DHCS &amp; CDSS Requirement</b>	<p>The organization must:</p> <ul style="list-style-type: none"> <li>a. Review the privileges assigned to organization-defined roles or classes of users to validate the need for such privileges; and</li> <li>b. Reassign or removes privileges, if necessary, to correctly reflect organizational mission/business needs.</li> </ul>
<b>Supplemental Guidance (from NIST 800-53)</b>	<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>
<b>Control Number</b>	AC-7
<b>Title</b>	Unsuccessful Logon Attempts
<b>DHCS &amp; CDSS Requirement</b>	<p>The organization must:</p> <ul style="list-style-type: none"> <li>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</li> <li>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.</li> </ul>
<b>Supplemental Guidance (from NIST 800-53)</b>	<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>
<b>Control Number</b>	AC-8
<b>Title</b>	System Use Notification
<b>DHCS &amp; CDSS Requirement</b>	<p>The organization must:</p> <ul style="list-style-type: none"> <li>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"> <li>1. Users are accessing a U.S. Government information system;</li> <li>2. Information system usage may be monitored, recorded, and subject to audit;</li> <li>3. Unauthorized use of the information system is prohibited and subject to criminal and civil penalties; and</li> <li>4. Use of the information system indicates consent to monitoring and recording;</li> </ul> </li> <li>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</li> <li>c. For publicly accessible systems: <ul style="list-style-type: none"> <li>1. Displays system use information organization-defined conditions, before granting further access;</li> </ul> </li> </ul>

	<ol style="list-style-type: none"> <li>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</li> <li>3. Includes a description of the authorized uses of the system.</li> </ol> <p>At a minimum, this can be done at initial logon and is not required for every logon.</p>
<b>Supplemental Guidance (from NIST 800-53)</b>	<p>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.</p>
<b>Control Number</b>	AC-11
<b>Title</b>	Session Lock
<b>DHCS &amp; CDSS Requirement</b>	<p>The organization's information system:</p> <ol style="list-style-type: none"> <li>a. Prevents further access to the system by initiating a session lock after 15 minutes or upon receiving a request from a user; and</li> <li>b. Retains the session lock until the user reestablishes access using established identification and authentication procedures.</li> </ol>
<b>Supplemental Guidance (from NIST 800-53)</b>	<p>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.</p>
<b>Control Number</b>	AC-17
<b>Title</b>	Remote Access
<b>DHCS &amp; CDSS Requirement</b>	<p>The organization must:</p> <ol style="list-style-type: none"> <li>a. Establish and document usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; and</li> <li>b. Authorize remote access to the information system prior to allowing such connections.</li> </ol>
<b>Supplemental Guidance (from NIST 800-53)</b>	<p>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). 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-</p>

	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.
--	---

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

<b>Control Number</b>	AR-3
<b>Title</b>	Privacy Requirements for Contractors and Service Providers
<b>DHCS &amp; CDSS Requirement</b>	<p>The organization must:</p> <ul style="list-style-type: none"> <li>a. Establish privacy roles, responsibilities, and access requirements for contractors and service providers; and</li> <li>b. Includes privacy requirements in contracts and other acquisition-related documents.</li> </ul>
<b>Supplemental Guidance (from NIST 800-53)</b>	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.

**3. Audit and Accountability (AU)**

<b>Control Number</b>	AU-1
<b>Title</b>	Audit and Accountability Policy and Procedures
<b>DHCS &amp; CDSS Requirement</b>	<p>The organization must:</p> <ul style="list-style-type: none"> <li>a. Develop, document, and disseminate to individuals and organizations that store, process, or transmit PII: <ul style="list-style-type: none"> <li>1. An audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and</li> <li>2. Procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls; and</li> </ul> </li> <li>b. Review and update the current: <ul style="list-style-type: none"> <li>1. Audit and accountability policy at least triennially; and</li> <li>2. Audit and accountability procedures at least triennially.</li> </ul> </li> </ul>
<b>Supplemental Guidance (from NIST 800-53)</b>	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.
<b>Control Number</b>	AU-2
<b>Title</b>	Audit Events
<b>DHCS &amp; CDSS Requirement</b>	<p>The organization must:</p> <ul style="list-style-type: none"> <li>a. Audit the following events:</li> </ul>

	<ol style="list-style-type: none"> <li>1. Viewing PII stored within the organization’s system;</li> <li>2. Viewing of screens that contain PII;</li> <li>3. All system and data interactions concerning PII.</li> </ol> <ol style="list-style-type: none"> <li>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;</li> <li>c. Determines that the following events are to be audited within the information system:             <ol style="list-style-type: none"> <li>1. Viewing PII stored within the organization’s system;</li> <li>2. Viewing of screens that contain PII;</li> <li>3. All system and data interactions concerning PII.</li> </ol> </li> </ol>
<b>Supplemental Guidance (from NIST 800-53)</b>	<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 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.</p> <p>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>
<b>Control Number</b>	AU-11
<b>Title</b>	Audit Record Retention
<b>DHCS &amp; CDSS Requirement</b>	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.
<b>Supplemental Guidance (from NIST 800-53)</b>	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.
<b>Control Number</b>	AU-12
<b>Title</b>	Audit Generation
<b>DHCS &amp; CDSS</b>	The organization information system must:

<b>Requirement</b>	<ul style="list-style-type: none"> <li>a. Provide audit record generation capability for the auditable events defined in AU-2 a. at the audit reporting mechanism;</li> <li>b. Allow security personnel to select which auditable events are to be audited by specific components of the information system; and</li> <li>c. Generates audit records for the events defined in AU-2 d. with the content defined in AU-3</li> </ul>
<b>Supplemental Guidance (from NIST 800-53)</b>	<p>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.</p>

4. **Awareness and Training (AT)**

<b>Control Number</b>	AT-1
<b>Title</b>	Security Awareness and Training Policy and Procedures
<b>DHCS &amp; CDSS Requirement</b>	<p>The organization must:</p> <ul style="list-style-type: none"> <li>a. Develop, document, and disseminate to personnel and organizations with access to PII: <ul style="list-style-type: none"> <li>1. A security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and</li> <li>2. Procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls; and</li> </ul> </li> <li>b. Reviews and updates the current: <ul style="list-style-type: none"> <li>1. Security awareness and training policy and;</li> <li>2. Security awareness and training procedures.</li> </ul> </li> </ul> <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>
<b>Supplemental Guidance (from NIST 800-53)</b>	<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</p>

	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.
<b>Control Number</b>	AT-2
<b>Title</b>	Security Awareness Training
<b>DHCS &amp; CDSS Requirement</b>	The organization must provide basic security awareness training to information system users (including managers, senior executives, and contractors): <ul style="list-style-type: none"> <li>a. As part of initial training for new users;</li> <li>b. When required by information system changes; and</li> <li>c. Annually thereafter.</li> </ul>
<b>Supplemental Guidance (from NIST 800-53)</b>	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.
<b>Control Number</b>	AT-3
<b>Title</b>	Role-Based Security Training
<b>DHCS &amp; CDSS Requirement</b>	The organization must provide role-based security training to personnel with assigned security roles and responsibilities: <ul style="list-style-type: none"> <li>a. Before authorizing access to the information system or performing assigned duties;</li> <li>b. When required by information system changes; and</li> <li>c. With organization-defined frequency thereafter.</li> </ul>
<b>Supplemental Guidance (from NIST 800-53)</b>	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.
<b>Control Number</b>	AT-4
<b>Title</b>	Security Training Records
<b>DHCS &amp; CDSS Requirement</b>	The organization must: <ul style="list-style-type: none"> <li>a. Document and monitor individual information system security training activities including basic security awareness training and specific information system security training; and</li> </ul>

	<p>b. Retain individual training records for 5 years.</p> <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>
<b>Supplemental Guidance (from NIST 800-53)</b>	<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)

Control Number	CP-2
<b>Title</b>	Contingency Plan
<b>DHCS &amp; CDSS Requirement</b>	<p>The organization must:</p> <ol style="list-style-type: none"> <li>a. Develop a contingency plan for the information system that:                             <ol style="list-style-type: none"> <li>1. Identifies essential missions and business functions and associated contingency requirements;</li> <li>2. Provides recovery objectives, restoration priorities, and metrics;</li> <li>3. Addresses contingency roles, responsibilities, assigned individuals with contact information;</li> <li>4. Addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure;</li> <li>5. Addresses eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented; and</li> <li>6. Is reviewed and approved by a senior manager;</li> </ol> </li> <li>b. Distribute copies of the contingency plan to personnel and organizations supporting the contingency plan actions;</li> <li>c. Coordinate contingency planning activities with incident handling activities;</li> <li>d. Review the contingency plan for the information system at least annually;</li> <li>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;</li> <li>f. Communicate contingency plan changes to personnel and organizations supporting the contingency plan actions;</li> <li>g. Incorporate lessons learned from contingency plan testing, training, or actual contingency activities into contingency testing and training; and</li> <li>h. Protect the contingency plan from unauthorized disclosure and modification.</li> </ol>
<b>Supplemental Guidance (from NIST 800-53)</b>	<p>Contingency planning for information systems is part of an overall organizational program for achieving continuity of operations for mission/business functions. Contingency planning 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,</p>

	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.
--	---

**6. Data Minimization and Retention (DM)**

<b>Control Number</b>	DM-2
<b>Title</b>	Data Retention and Disposal
<b>DHCS &amp; CDSS Requirement</b>	<p>The organization must:</p> <ul style="list-style-type: none"> <li>a. Retain each collection of PII no longer than required for the organization’s business process or evidentiary purposes;</li> <li>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</li> <li>c. Use organization-defined techniques or methods to ensure secure deletion or destruction of PII (including originals, copies, and archived records).</li> </ul>
<b>Supplemental Guidance (from NIST 800-53)</b>	<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.</p> <p>Certain read-only archiving techniques, such as DVDs, CDs, microfilm, or microfiche, may 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.</p>

**7. Identification and Authentication (IA)**

<b>Control Number</b>	IA-2
<b>Title</b>	Identification and Authentication (Organizational Users)
<b>DHCS &amp; CDSS Requirement</b>	The organization's information system must uniquely identify and authenticate organizational users (or processes acting on behalf of organizational users).
<b>Supplemental Guidance (from NIST 800-53)</b>	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

	<p>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>
<b>Control Number</b>	IA-5
<b>Title</b>	Authenticator Management
<b>DHCS &amp; CDSS Requirement</b>	<p>The organization must manage information system authenticators by:</p> <ol style="list-style-type: none"> <li>a. Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, or device receiving the authenticator;</li> <li>b. Establishing initial authenticator content for authenticators defined by the organization;</li> <li>c. Ensuring that authenticators have sufficient strength of mechanism for their intended use;</li> <li>d. Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators;</li> <li>e. Changing default content of authenticators prior to information system installation;</li> <li>f. Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators;</li> <li>g. Changing/refreshing authenticators within organization-defined time period;</li> <li>h. Protecting authenticator content from unauthorized disclosure and modification;</li> <li>i. Requiring individuals to take, and having devices implement, specific security safeguards to protect authenticators; and</li> <li>j. Changing authenticators for group/role accounts when membership to those accounts changes.</li> </ol>
<b>Supplemental Guidance (from</b>	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

<b>NIST 800-53)</b>	<p>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>
<b>Control Number</b>	IA-5(1)
<b>Title</b>	Authenticator Management   Password-Based Authentication
<b>DHCS &amp; CDSS Requirement</b>	<p>The information system, for password-based authentication, must:</p> <ul style="list-style-type: none"> <li>a. Enforces minimum password complexity of requirements for: <ul style="list-style-type: none"> <li>* case sensitivity (upper and lower case letters),</li> <li>* number of characters (equal to or greater than fifteen characters),</li> <li>* mix of upper-case letters, lower-case letters, numbers, and special characters (at least one of each type);</li> </ul> </li> <li>c. Stores and transmits only cryptographically-protected passwords;</li> <li>d. Enforces password lifetime of at least 180 days;</li> <li>e. Prohibits prior 10 passwords for reuse; and</li> <li>f. Allows the use of a temporary password for system logons with an immediate change to a permanent password.</li> </ul>
<b>Supplemental Guidance (from NIST 800-53)</b>	<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)**

<b>Control Number</b>	IR-1
-----------------------	------

<b>Title</b>	Incident Response Policy and Procedures
<b>DHCS &amp; CDSS Requirement</b>	<p>The organization must:</p> <ul style="list-style-type: none"> <li>a. Develops, documents, and disseminates to organization-defined personnel or roles: <ul style="list-style-type: none"> <li>1. An incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and</li> <li>2. Procedures to facilitate the implementation of the incident response policy and associated incident response controls; and</li> </ul> </li> <li>b. Reviews and updates the current: <ul style="list-style-type: none"> <li>1. Incident response policy with organization-defined frequency; and</li> <li>2. Incident response procedures with organization-defined frequency.</li> </ul> </li> </ul> <p><i>DHCS, CDSS and NIST Guidelines encourage agencies to consider establishing incident response teams or identifying individuals specifically responsible for addressing PII, DHCS and CDSS data breaches.</i></p>
<b>Supplemental Guidance (from NIST 800-53)</b>	<p>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.</p>
<b>Control Number</b>	IR-2
<b>Title</b>	Incident Response Training
<b>DHCS &amp; CDSS Requirement</b>	<p>The organization must provide incident response training to information system users consistent with assigned roles and responsibilities:</p> <ul style="list-style-type: none"> <li>a. Within organization-defined time period of assuming an incident response role or responsibility;</li> <li>b. When required by information system changes; and</li> <li>c. With organization-defined frequency thereafter.</li> </ul>
<b>Supplemental Guidance (from NIST 800-53)</b>	<p>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.</p>
<b>Control Number</b>	IR-4
<b>Title</b>	Incident Handling
<b>DHCS &amp; CDSS Requirement</b>	<p>The organization must:</p> <ul style="list-style-type: none"> <li>a. Implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery;</li> <li>b. Coordinates incident handling activities with contingency planning activities; and</li> <li>c. Incorporates lessons learned from ongoing incident handling activities into incident response</li> </ul>

	procedures, training, and testing, and implements the resulting changes accordingly.
<b>Supplemental Guidance (from NIST 800-53)</b>	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.
<b>Control Number</b>	IR-8
<b>Title</b>	Incident Response Plan
<b>DHCS &amp; CDSS Requirement</b>	<p>The organization must:</p> <ol style="list-style-type: none"> <li>a. Develop an incident response plan that: <ol style="list-style-type: none"> <li>1. Provides the organization with a roadmap for implementing its incident response capability;</li> <li>2. Describes the structure and organization of the incident response capability;</li> <li>3. Provides a high-level approach for how the incident response capability fits into the overall organization;</li> <li>4. Meets the unique requirements of the organization, which relate to mission, size, structure, and functions;</li> <li>5. Defines reportable incidents;</li> <li>6. Provides metrics for measuring the incident response capability within the organization;</li> <li>7. Defines the resources and management support needed to effectively maintain and mature an incident response capability; and</li> <li>8. Is reviewed and approved by organization-defined personnel or roles;</li> </ol> </li> <li>b. Distribute copies of the incident response plan to organization-defined incident response personnel (identified by name and/or by role) and organizational elements;</li> <li>c. Review the incident response plan organization-defined frequency;</li> <li>d. Updates the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing;</li> <li>e. Communicate incident response plan changes to organization-defined incident response personnel (identified by name and/or by role) and organizational elements]; and</li> <li>f. Protect the incident response plan from unauthorized disclosure and modification.</li> </ol>
<b>Supplemental Guidance (from NIST 800-53)</b>	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)**

<b>Control Number</b>	MP-2
-----------------------	------

<b>Title</b>	Media Access
<b>DHCS &amp; CDSS Requirement</b>	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.
<b>Supplemental Guidance (from NIST 800-53)</b>	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.
<b>Control Number</b>	MP-6
<b>Title</b>	Media Sanitization
<b>DHCS &amp; CDSS Requirement</b>	The organization must: <ul style="list-style-type: none"> <li>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</li> <li>b. Employs sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.</li> </ul>
<b>Supplemental Guidance (from NIST 800-53)</b>	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)

<b>Control Number</b>	PS-3
<b>Title</b>	Personnel Screening
<b>DHCS &amp; CDSS Requirement</b>	The organization must: <ul style="list-style-type: none"> <li>a. Screen individuals (employees, contractors and agents) prior to authorizing access to the information system and PII.</li> </ul>
<b>Supplemental Guidance (from NIST 800-53)</b>	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.
<b>Control Number</b>	PS-4
<b>Title</b>	Personnel Termination
<b>DHCS &amp; CDSS Requirement</b>	The organization, upon termination of individual employment, must: <ol style="list-style-type: none"> <li>a. Disable information system access;</li> <li>b. Terminate/revoke any authenticators/credentials associated with the individual;</li> <li>c. Conduct exit interviews, as needed;</li> <li>d. Retrieve all security-related organizational information system-related property;</li> <li>e. Retain access to organizational information and information systems formerly controlled by terminated individual; and</li> <li>f. Notified organization-defined personnel upon termination.</li> </ol>
<b>Supplemental Guidance (from NIST 800-53)</b>	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.
<b>Control Number</b>	PS-6
<b>Title</b>	Access Agreements
<b>DHCS &amp; CDSS Requirement</b>	The organization must: <ol style="list-style-type: none"> <li>a. Develop and document access agreements for organizational information systems;</li> <li>b. Reviews and updates the access agreements at organization-defined frequency; and</li> <li>c. Ensure that individuals requiring access to organizational information and information systems:                         <ol style="list-style-type: none"> <li>1. Sign appropriate access agreements prior to being granted access; and</li> <li>2. Re-sign access agreements to maintain access to organizational information systems when access agreements have been updated or at an organization-defined frequency.</li> </ol> </li> </ol> 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.
<b>Supplemental Guidance (from NIST 800-53)</b>	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.
<b>Control Number</b>	PS-7
<b>Title</b>	Third-Party Personnel Security
<b>DHCS &amp; CDSS</b>	The organization must:

<p><b>Requirement</b></p>	<ul style="list-style-type: none"> <li>a. Establishes personnel security requirements including security roles and responsibilities for county agents, subcontractors, and vendors;</li> <li>b. Requires third-party providers to comply with personnel security policies and procedures established by the organization;</li> <li>c. Documents personnel security requirements;</li> <li>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</li> <li>e. Monitors provider compliance.</li> </ul> <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> <ul style="list-style-type: none"> <li>1. <i>General Use of PII;</i></li> <li>2. <i>Security and Privacy Safeguards for PII;</i></li> <li>3. <i>Unacceptable Use of PII; and</i></li> <li>4. <i>Enforcement Policies.</i></li> </ul> <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>
<p><b>Supplemental Guidance (from NIST 800-53)</b></p>	<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 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.</p>
<p><b>Control Number</b></p>	<p>PS-8</p>
<p><b>Title</b></p>	<p>Personnel Sanctions</p>
<p><b>DHCS &amp; CDSS Requirement</b></p>	<p>The organization must:</p> <ul style="list-style-type: none"> <li>a. Employ a formal sanctions process for individuals failing to comply with established information security policies and procedures; and</li> <li>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.</li> </ul> <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>
<p><b>Supplemental Guidance (from NIST 800-53)</b></p>	<p>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.</p>

11. Physical and Environmental Protection (PE)

<b>Control Number</b>	PE-3
<b>Title</b>	Physical Access Control
<b>DHCS &amp; CDSS Requirement</b>	<p>The organization must:</p> <ul style="list-style-type: none"> <li>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"> <li>1. Verifying individual access authorizations before granting access to the facility; and</li> <li>2. Controlling ingress/egress to the facility using physical access control systems/devices and/or guards;</li> </ul> </li> <li>b. Maintain physical access audit logs for entry and exit points;</li> <li>c. Provide security safeguards to control access to areas within the facility officially designated as publicly accessible;</li> <li>d. Escort visitors and monitors visitor activity;</li> <li>e. Secure keys, combinations, and other physical access devices;</li> <li>f. Inventory physical access devices; and</li> <li>g. Changes combinations and keys at minimum when keys are lost, combinations are compromised, or individuals are transferred or terminated</li> </ul>
<b>Supplemental Guidance (from NIST 800-53)</b>	<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. 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>
<b>Control Number</b>	PE-6
<b>Title</b>	Monitoring Physical Access
<b>DHCS &amp; CDSS Requirement</b>	<p>The organization must:</p> <ul style="list-style-type: none"> <li>a. Monitors physical access to the facility where the information system resides to detect and respond to physical security incidents;</li> <li>b. Reviews physical access logs organization-defined frequency and upon occurrence of security incidents; and</li> <li>c. Coordinates results of reviews and investigations with the organizational incident response capability.</li> </ul>
<b>Supplemental</b>	Organizational incident response capabilities include investigations of and responses to detected

<b>Guidance (from NIST 800-53)</b>	<p>physical security incidents. Security incidents include, for example, apparent security violations or suspicious physical access activities. Suspicious physical access activities include, for example:</p> <ul style="list-style-type: none"> <li>(i) accesses outside of normal work hours;</li> <li>(ii) repeated accesses to areas not normally accessed;</li> <li>(iii) accesses for unusual lengths of time; and (iv) out-of-sequence accesses.</li> </ul> <p>Related controls: CA-7, IR-4, IR-8.</p>
------------------------------------	---

12. **Planning (PL)**

<b>Control Number</b>	PL-1
<b>Title</b>	Security Planning Policy and Procedures
<b>DHCS &amp; CDSS Requirement</b>	<p>The organization must:</p> <ul style="list-style-type: none"> <li>a. Develop, document, and disseminate to personnel and organizations with access to PII: <ul style="list-style-type: none"> <li>1. A security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and</li> <li>2. Procedures to facilitate the implementation of the security planning policy and associated security planning controls; and</li> </ul> </li> <li>b. Reviews and updates the current: <ul style="list-style-type: none"> <li>1. Security planning policy; and</li> <li>2. Security planning procedures.</li> </ul> </li> </ul>
<b>Supplemental Guidance (from NIST 800-53)</b>	<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>
<b>Control Number</b>	PL-2
<b>Title</b>	System Security Plan
<b>DHCS &amp; CDSS Requirement</b>	<p>The organization must:</p> <ul style="list-style-type: none"> <li>a. Develop a security plan for the information system that: <ul style="list-style-type: none"> <li>1. Is consistent with the organization’s enterprise architecture;</li> <li>2. Explicitly defines the authorization boundary for the system;</li> <li>3. Describes the operational context of the information system in terms of missions and business processes;</li> <li>4. Provides the security categorization of the information system including supporting rationale;</li> <li>5. Describes the operational environment for the information system and relationships with or connections to other information systems;</li> <li>6. Provides an overview of the security requirements for the system;</li> <li>7. Identifies any relevant overlays, if applicable;</li> <li>8. Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring decisions; and</li> </ul> </li> </ul>

	<p>9. Is reviewed and approved by the authorizing official or designated representative prior to plan implementation;</p> <p>b. Distribute copies of the security plan and communicates subsequent changes to the plan to personnel and organizations with security responsibilities;</p> <p>c. Review the security plan for the information system;</p> <p>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</p> <p>e. Protect the security plan from unauthorized disclosure and modification.</p> <p><i>Organization's security plan should include detailed information specific to safeguarding Medi- Cal PII.</i></p>
<p><b>Supplemental Guidance (from NIST 800-53)</b></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><b>Control Number</b></p>	<p>RA-1</p>
<p><b>Title</b></p>	<p>Risk Assessment Policy and Procedures</p>
<p><b>DHCS &amp; CDSS Requirement</b></p>	<p>The organization must:</p> <p>a. Develop, document, and disseminate to system owners using PII:</p> <ol style="list-style-type: none"> <li>1. A risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and</li> <li>2. Procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls.</li> </ol>
<p><b>Supplemental Guidance (from NIST 800-53)</b></p>	<p>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-</p>

	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.
<b>Control Number</b>	RA-3
<b>Title</b>	Risk Assessment
<b>DHCS &amp; CDSS Requirement</b>	<p>The organization must:</p> <ol style="list-style-type: none"> <li>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;</li> <li>b. Documents risk assessment results in a risk assessment report or organization defined risk report document.</li> <li>c. Review risk assessment results annually; and</li> <li>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.</li> </ol>
<b>Supplemental Guidance (from NIST 800-53)</b>	<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>
<b>Control Number</b>	RA-5
<b>Title</b>	Vulnerability Scanning
<b>DHCS &amp; CDSS Requirement</b>	<p>The organization must:</p> <ol style="list-style-type: none"> <li>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;</li> <li>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"> <li>1. Enumerating platforms, software flaws, and improper configurations;                 <ol style="list-style-type: none"> <li>a. Analyze vulnerability scan reports and results from security control assessments;</li> <li>b. Remediate legitimate vulnerabilities within organization defined time periods in</li> </ol> </li> </ol> </li> </ol>

	<p>accordance with an organizational assessment of risk; and</p> <p>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).</p>
<p><b>Supplemental Guidance (from NIST 800-53)</b></p>	<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)**

<p><b>Control Number</b></p>	<p>CA-2</p>
<p><b>Title</b></p>	<p>Security Assessments</p>
<p><b>DHCS &amp; CDSS Requirement</b></p>	<p>The organization must:</p> <ul style="list-style-type: none"> <li>a. Develops a security assessment plan that describes the scope of the assessment including:             <ul style="list-style-type: none"> <li>1. Security controls and control enhancements under assessment;</li> <li>2. Assessment procedures to be used to determine security control effectiveness; and</li> <li>3. Assessment environment, assessment team, and assessment roles and responsibilities;</li> </ul> </li> <li>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;</li> <li>c. Produces a security assessment report that documents the results of the assessment; and</li> <li>d. Provides the results of the security control assessment to organization-defined individuals or roles.</li> </ul>
<p><b>Supplemental Guidance (from NIST 800-53)</b></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</p>

	<p>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>
<b>Control Number</b>	CA-3
<b>Title</b>	System Interconnections
<b>DHCS &amp; CDSS Requirement</b>	<p>The organization must:</p> <ul style="list-style-type: none"> <li>a. Authorizes connections from the information system to other information systems through the use of Interconnection Security Agreements;</li> <li>b. Documents, for each interconnection, the interface characteristics, security requirements, and the nature of the information communicated; and</li> <li>c. Reviews and updates Interconnection Security Agreements [Assignment: organization-defined frequency].</li> </ul>
<b>Supplemental Guidance (from NIST 800-53)</b>	<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>

<b>Control Number</b>	CA-7
<b>Title</b>	Continuous Monitoring
<b>DHCS &amp; CDSS Requirement</b>	<p>The organization must develop a continuous monitoring strategy and implement a continuous monitoring program that includes:</p> <ul style="list-style-type: none"> <li>a. Establishment of PII security controls to be monitored;</li> <li>c. Ongoing security control assessments in accordance with the organizational continuous monitoring strategy;</li> <li>d. Ongoing security status monitoring of PII security controls in accordance with the organizational continuous monitoring strategy;</li> <li>e. Correlation and analysis of security-related information generated by assessments and monitoring;</li> <li>f. Response actions to address results of the analysis of security-related information; and</li> <li>g. Reporting the security status of organization and the information system to organization- defined personnel or roles and to DHCS and CDSS when requested.</li> </ul>
<b>Supplemental Guidance (from NIST 800-53)</b>	<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.</p> <p>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.</p> <p>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.</p> <p>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>
<b>Control Number</b>	CA-8
<b>Title</b>	Penetration Testing
<b>DHCS &amp; CDSS Requirement</b>	<p>The organization must conduct penetration testing annually on systems storing, processing, or transmitting PII.</p>
<b>Supplemental Guidance (from NIST 800-53)</b>	<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"> <li>(i) pretest analysis based on full knowledge of the target system;</li> <li>(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</li> </ul>

	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)**

<b>Control Number</b>	SC-7
<b>Title</b>	Boundary Protection
<b>DHCS &amp; CDSS Requirement</b>	The organization information system must: <ul style="list-style-type: none"> <li>a. Monitor and control communications at the external boundary of the system and at key internal boundaries within the system;</li> <li>b. Implements subnetworks for publicly accessible system components that are physically and logically separated from internal organizational networks; and</li> <li>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.</li> </ul>
<b>Supplemental Guidance (from NIST 800-53)</b>	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.  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.
<b>Control Number</b>	SC-8
<b>Title</b>	Transmission Confidentiality and Integrity
<b>DHCS &amp; CDSS Requirement</b>	The organization information system must: Protect the confidentiality of transmitted information.
<b>Supplemental Guidance (from NIST 800-53)</b>	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.

	Related controls: AC-17, PE-4.
<b>Control Number</b>	SC-8(1)
<b>Title</b>	Transmission Confidentiality and Integrity   Cryptographic or Alternate Physical Protection
<b>DHCS &amp; CDSS Requirement</b>	The organization information system must implement cryptographic mechanisms to prevent unauthorized disclosure of information during transmission.
<b>Supplemental Guidance (from NIST 800-53)</b>	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.
<b>Control Number SC-13</b>	Control Number SC-13
<b>Title</b>	Cryptographic Protection
<b>CDSS Requirement</b>	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.
<b>Supplemental Guidance (from NIST 800-53)</b>	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.
<b>Control Number</b>	SC-28
<b>Title</b>	Protection of Information at Rest
<b>DHCS &amp; CDSS Requirement</b>	The organization information system must: Protect the confidentiality of PII at rest.
<b>Supplemental Guidance (from NIST 800-53)</b>	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)

<b>Control Number</b>	SI-2
-----------------------	------

<b>Title</b>	Flaw Remediation
<b>DHCS &amp; CDSS Requirement</b>	<p>The organization must:</p> <ol style="list-style-type: none"> <li>a. Identify, report, and correct information system flaws;</li> <li>b. Tests software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation;</li> <li>c. Installs security-relevant software and firmware updates, within acceptable organization standards, of the release of the updates; and</li> <li>d. Incorporates flaw remediation into the organizational configuration management process.</li> </ol>
<b>Supplemental Guidance (from NIST 800-53)</b>	<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.</p> <p>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.</p> <p>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>
<b>Control Number</b>	SI-3
<b>Title</b>	Malicious Code Protection
<b>DHCS &amp; CDSS Requirement</b>	<p>The organization must:</p> <ol style="list-style-type: none"> <li>a. Employ malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code;</li> <li>b. Update malicious code protection mechanisms whenever new releases are available in accordance with organizational configuration management policy and procedures;</li> <li>c. Configure malicious code protection mechanisms to:             <ol style="list-style-type: none"> <li>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</li> <li>2. Block malicious code or quarantine malicious code, and send alert to administrator for incident handling in response to malicious code detection; and</li> </ol> </li> <li>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</li> </ol>
<b>Supplemental Guidance (from</b>	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.

<p><b>NIST 800-53)</b></p>	<p>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><b>Control Number</b></p>	<p>SI-4</p>
<p><b>Title</b></p>	<p>Information System Monitoring</p>
<p><b>DHCS &amp; CDSS Requirement</b></p>	<p>The organization must:</p> <ul style="list-style-type: none"> <li>a. Monitor the information system to detect:             <ul style="list-style-type: none"> <li>1. Attacks and indicators of potential attacks in accordance with organization-defined monitoring objectives; and</li> <li>2. Unauthorized local, network, and remote connections;</li> </ul> </li> <li>b. Identify unauthorized use of the information system through organization-defined techniques and methods;</li> <li>c. Deploy monitoring devices:             <ul style="list-style-type: none"> <li>1. Strategically within the information system to collect organization-determined essential information; and</li> <li>2. At ad hoc locations within the system to track specific types of transactions of interest to the organization;</li> </ul> </li> <li>d. Protect information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion;</li> <li>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.</li> <li>f. Obtain legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations; and</li> <li>g. Provides organization-defined information system monitoring information to organization- defined personnel and DHCS and CDSS as needed.</li> </ul>
<p><b>Supplemental Guidance (from</b></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</p>

<b>NIST 800-53)</b>	<p>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.</p> <p>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>
<b>Control Number</b>	SI-4(5)
<b>Title</b>	Information System Monitoring   System Generated Alerts
<b>DHCS &amp; CDSS Requirement</b>	<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"> <li>1. Protected system files or directories have been modified without notification from the appropriate change/configuration management channels.</li> <li>2. System performance indicates resource consumption that is inconsistent with expected operating conditions.</li> <li>3. Auditing functionality has been disabled or modified to reduce audit visibility.</li> <li>4. Audit or log records have been deleted or modified without explanation.</li> <li>5. The system is raising alerts or faults in a manner that indicates the presence of an abnormal condition.</li> <li>6. Resource or service requests are initiated from clients that are outside of the expected client membership set.</li> <li>7. The system reports failed logins or password changes for administrative or key service accounts.</li> <li>8. Processes and services are running that are outside of the baseline system profile.</li> <li>9. Utilities, tools, or scripts have been saved or installed on production systems without clear indication of their use or purpose.</li> </ol>
<b>Supplemental Guidance (from NIST 800-53)</b>	<p>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.</p>
<b>Control Number</b>	SI-4(13)
<b>Title</b>	Information System Monitoring   Analyze Traffic / Event Patterns
<b>DHCS &amp; CDSS Requirement</b>	<p>The organization must:</p> <ol style="list-style-type: none"> <li>a. Analyzes communications traffic/event patterns for the information system;</li> <li>b. Develops profiles representing common traffic patterns and/or events; and</li> </ol>

	c. Uses the traffic/event profiles in tuning system-monitoring devices to reduce the number of false positives and the number of false negatives.
<b>Supplemental Guidance (from NIST 800-53)</b>	None

**17. System and Services Acquisition (SA)**

<b>Control Number</b>	<b>SA-9</b>
<b>Title</b>	External Information System Services
<b>DHCS &amp; CDSS Requirement</b>	<p>The organization must:</p> <ul style="list-style-type: none"> <li>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;</li> <li>b. Defines and documents government oversight and user roles and responsibilities with regard to external information system services; and</li> <li>c. Employs organization-defined processes, methods, and techniques to monitor security control compliance by external service providers on an ongoing basis.</li> </ul> <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>
<b>Supplemental Guidance (from NIST 800-53)</b>	<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>
<b>Control Number</b>	<b>SA-11</b>
<b>Title</b>	Developer Security Testing And Evaluation
<b>DHCS &amp; CDSS Requirement</b>	The organization must require the developer of the information system, system component, or information system service to:

	<ul style="list-style-type: none"> <li>a. Create and implement a security assessment plan;</li> <li>b. Perform [Selection (one or more): unit; integration; system; regression] testing/evaluation at [Assignment: organization-defined depth and coverage];</li> <li>c. Produce evidence of the execution of the security assessment plan and the results of the security testing/evaluation;</li> <li>d. Implement a verifiable flaw remediation process; and</li> <li>e. Correct flaws identified during security testing/evaluation</li> </ul>
<p><b>Supplemental Guidance (from NIST 800-53)</b></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>

[Remainder of page intentionally left blank]

**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 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 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 **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**

Andrew Alipanah, MBA, CISSP  
 Chief Information Security Officer  
 County of Orange  
 Enterprise Privacy & Cybersecurity

721 S. Parker St., Ste. 200  
 Orange, CA 92868

Email: Andrew.Alipanah@ocit.oc.gov

Telephone: (714) 567-7611

Linda Le, CHC, CHPC, CHP  
 County Privacy Officer  
 County of Orange  
 Enterprise Privacy & Cybersecurity

721 S. Parker St., Suite 200  
 Orange, CA 92868

Email: privacyofficer@ocgov.com  
 securityadmin@ocit.oc.gov  
 linda.le@ocit.oc.gov

Telephone: (714) 834-4082

<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: <a href="mailto:Karen.vu@ssa.ocgov.com">Karen.vu@ssa.ocgov.com</a></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: <a href="mailto:Alin.buna@ssa.ocgov.com">Alin.buna@ssa.ocgov.com</a></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.*

<p><b>PSA Inquiries and Questions</b></p> <p>County of Orange Social Services Agency 500 N. State College Blvd. Orange, CA 92868</p> <p>Email: <a href="mailto:ssacontractsservices@ssa.ocgov.com">ssacontractsservices@ssa.ocgov.com</a></p>
---

**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.