# MEMORANDUM OF UNDERSTANDING
# BETWEEN
# THE COUNTY OF ORANGE SOCIAL SERVICES AGENCY
# AND
# CHILDREN AND FAMILIES COMMISSION OF ORANGE COUNTY
# AND
# ASIAN AMERICAN SENIOR CITIZENS SERVICE CENTER, INC.
# TO ESTABLISH A MULTIDISCIPLINARY PERSONNEL TEAM
# FOR THE PROVISION OF
# NEIGHBORHOOD RESOURCE NETWORK SERVICES

This Memorandum of Understanding (MOU) is entered into by and between the County of Orange, acting through its Social Services Agency (SSA), hereinafter referred to as "County," the Children and Families Commission of Orange County, hereinafter referred to as "First 5 Orange County," and Asian American Senior Citizens Service Center, Inc., hereinafter referred to as "CBO." This MOU provides guidelines for the establishment of a Multidisciplinary Team (MDT) for child abuse prevention and intervention efforts through the provision of Neighborhood Resource Network (NRN) Services.

County, First 5 Orange County, and CBO may be referred to individually as "Party" and collectively as "the Parties." The relationship between County, First 5 Orange County, and CBO, with regard to this MOU, is based upon the following:

1. This MOU is authorized and provided for pursuant to California Welfare and Institutions Code (WIC) Sections 10850.1, 18951 and 18961.7, which outline the requirements for the formation and implementation of a MDT, and WIC Section 10601.2, which establishes the parameters for county assessment of best practices to achieve performance outcome indicators for child welfare programs.
2. The Parties agree to work together and follow the requirements set forth in this MOU to provide NRN services through the MDT as defined in WIC 18951(d), which is engaged in the prevention, identification, management, or treatment of child abuse or neglect.

3. County provides services for the provision of child abuse and neglect prevention and intervention services as authorized and provided for pursuant to WIC Section 16501.
4. An agreement between County, First 5 Orange County, and CBO to establish and engage an MDT for child abuse prevention and intervention through the provision of NRN services will engage a greater number of families in services within the community without bringing those families into the child welfare system.
5. This non-financial MOU is a legally binding agreement based on the promises of the Parties.

TABLE OF CONTENTS

1. TERM

The term of this MOU shall commence on July 1, 2026, and end on June 30, 2029, unless earlier terminated pursuant to the provisions of Paragraph 25 of this MOU; however, the Parties shall be obligated to perform such duties as would normally extend beyond this term, including, but not limited to, obligations with respect to indemnification, reporting and confidentiality.

2. DEFINITIONS

2.1 Child Abuse Hotline: A 24-hour hotline for reporting suspected child abuse.

2.2 Child Abuse Report: A formal, confidential document filed by a mandated reporter or other citizen that alleges suspected child abuse or neglect.

2.3 Differential Response Tracking System (DRTS): A computerized system designed to record and manage information received from calls or reports related to child maltreatment.

2.4 Healthy Families America (HFA): A national, evidence-based program providing free, voluntary home visiting to support pregnant people and new parents, helping them build strong parent-child relationships, learn about child development, access resources, and prevent child abuse/neglect by fostering nurturing family environments through strength-based, culturally sensitive support.

2.5 Multidisciplinary Team (MDT): Pursuant to WIC Section 18951, an MDT is a team of three or more persons trained in the prevention, identification, management or treatment of child abuse and neglect cases and who are qualified to provide a broad range of services related to child abuse or neglect.

2.6 Parent Child Interaction Therapy (PCIT): An evidence-based treatment for young children with disruptive behaviors that focuses on strengthening the parent-child relationship while teaching caregivers how to manage behavior in a supportive, consistent way.

2.7 Parents As Teachers (PAT): Evidence-based, home-visiting program model that supports parents and caregivers to promote early childhood development.

3. POPULATION TO BE SERVED

3.1 Children and families who have had a child abuse report and are referred to the program by County. NRN services shall be provided to families that meet all of the following criteria:

3.1.1 Families for which this is the first Child Abuse Report;

3.1.2 Families with one or more children in the household with ages from birth through five years of age; and

3.1.3 Families whose Child Abuse Report has been investigated and will not receive further intervention by County, including those that are not substantiated due to not meeting the legal threshold for further intervention based on the determination by County.

4. PURPOSE AND GOAL

4.1 The purpose of this MOU is to set forth provisions for the establishment of a MDT that is a collaboration between County, CBO, and First 5 Orange County, pursuant to the requirements of WIC Section 10850.1 and Penal Code Section 11167.5 that permits the disclosure and exchange of confidential information with other members of the MDT.

4.2 NRN services supports children and families to help reduce the risk of stressful situations in the home resulting in a Child Abuse Report to the Orange County Social Services Child Abuse Hotline. The purpose of NRN is to help create a voluntary support structure for families by connecting them to community services to help manage circumstances that create stress on families, thereby reducing the potential for child abuse.

4.3 The goal of this MOU is to prevent child abuse and neglect by engaging a greater number of families through the receipt of and participation in services that may be available within their community. Early identification and implementation of these community services will enhance the families' ability to become more self-sufficient and improve their parenting skills.

5. PROGRAM OUTCOMES

5.1 First 5 Orange County will assign a minimum of 90 percent of referrals to CBO within two business days of DRTS assignment.

5.2 CBO will attempt first contact for a minimum of 90 percent of referrals within three business days of First 5 Orange County assignment.

6. CBO AND FIRST 5 ORANGE COUNTY RESPONSIBILITIES

6.1 CBO shall:

6.1.1 Assess the needs of families referred to CBO by County and First Five Orange County.

6.1.2 Contact referred NRN families within three business days as established by County and First 5 Orange County, or until the family declines services.

6.1.2.1 County shall be notified of families that were unable to be contacted or contacted but declined voluntary services.

6.1.2.2 County shall be notified of families who initially decline services but accept at a later date.

6.1.3 Coordinate and perform a minimum of four outreach attempts to referred NRN families.

6.1.3.1 The procedure for complying with family outreach attempts shall be determined by County and First 5 Orange County.

6.1.3.2 Engagement of the family in the NRN Program occurs when the family accepts services.

6.1.4 Provide child abuse prevention and intervention services such as HFA, PAT and PCIT, or other similar evidence-based family strengthening services.

6.1.5 Contribute informational resources to assist in the sustainability of the MDT.

6.1.6 Possess knowledge of and experience with accessing and/or providing community resources.

6.1.7 Collaborate with other CBOs to create the MDT.

6.1.8 Conduct Live Scans for MDT members, as applicable and appropriate for the services under this MOU.

6.1.8.1 If transporting clients, the MDT member must provide a certified DMV copy of their driving record.

6.1.8.2 If the MDT member transports a child/children, the child/children must be accompanied by a parent, legal guardian, or other adult designated by a parent.

6.1.9 Maintain records of efforts or engagements to offer services, engagement outcomes, and other activities relevant to NRN as requested by County and First 5 Orange County. All information shall be documented in DRTS.

6.2 First 5 Orange County shall:

6.2.1 Facilitate, coordinate, schedule and/or participate in MDT meetings scheduled monthly or as agreed upon by members of the MDT.

6.2.2 Participate in MDT and related meetings with County and CBO to discuss information regarding families, review assessments, collaborate on service plan recommendations, and develop additional options for community-based service.

6.3 CBO and First 5 Orange County shall:

6.3.1 Submit a certification to County, in the form attached hereto as Exhibit A, representing that the MDT member received the training described in Subparagraphs 6.3.2, 6.3.3, and 7.6.

6.3.2 Provide training to MDT members, as requested by County and other parties to this MOU, in areas including but not limited to:

6.3.2.1 Rules of confidentiality that apply to this MOU and the MDT.

6.3.2.2 Usage of Differential Response Tracking System (DRTS).

6.3.2.3 Evidence based family strengthening programs, including but not limited to HFA, PAT, and PCIT.

6.3.3 Participate in any MDT or NRN related training, as requested by County.

6.3.4 Identify additional MDT members. The newly identified MDT members should be referred to County for member certification in accordance with Subparagraph 6.3.1 of this MOU.

6.3.5 As an MDT member, gather family information from County and evaluate for appropriateness of providing NRN services.

7. COUNTY RESPONSIBILITIES.

County shall:

7.1 Provide to MDT any and all Child Abuse Hotline information on children and families that meet NRN criteria, as permitted by WIC Sections 10850.1 and 18951, and Penal Code 11167.5.

7.1.1 At a minimum, the referral information must have the family's name and telephone number.

7.1.2 As a preferred standard business practice, all family referral information should include the following: name, telephone number, address, family make-up, demographics including but not limited to preferred language and tribal affiliation, and CalWORKS eligibility, where applicable.

7.2 Provide determination for Immediate/Ten Day/Emergency Response Investigations. Based on the Child Abuse Report, County may deem further investigation is necessary. If the investigation is determined inconclusive, unfounded, or substantiated and the case is closed, the family is deemed eligible for NRN services if:

7.2.1 The family will not receive further services;

7.2.2 There is a child age birth through five in the family; and

7.2.3 This is the first Child Abuse Report.

7.3 Create a report once a week of all closed eligible cases. County shall enter the group of eligible NRN families into the DRTS system for referral to CBOs.

7.4 Refer eligible NRN families to the most appropriate CBO(s) based on a referral process established by County and First 5 Orange County.

7.4.1 The referral process shall have timelines and engagement strategies that CBOs are required to comply with as members of the MDT.

7.4.2 Lists with eligible referrals shall be provided to First 5 Orange County on a weekly basis.

7.5 Indicate in DRTS whether the family is eligible for CalWORKs.

7.6 Ensure that MDT members complete required training and any MDT or NRN related training as requested by County.

7.7 Maintain copies of signed certifications referenced in Subparagraph 6.3.1.

7.8 Maintain records of Child Abuse Report information provided to the MDT.

7.9 Maintain records of the MDT's efforts and engagements for offering services to families, engagement and enrollment outcomes, and other activities relevant to NRN as reported by the MDT.

7.10 Collect, compare, and analyze data on families that successfully complete NRN to Child Abuse Hotline data. This comparison analysis is to be completed in six-month intervals.

8. FACILITIES:

8.1 It is mutually understood that CBO will provide services at the following facilities:

Asian American Senior Citizens Service Center, Inc.
850 N. Birch Street
Santa Ana, CA 92701

8.2 It is mutually understood that First 5 Orange County will provide services at the following facilities:

First 5 Orange County
1505 East 17th Street
Santa Ana, CA 92705

8.3 CBO, First 5 Orange County, and County may mutually agree in writing to add, change, modify, or delete facility location(s) as necessary to best serve the needs of County and families to be served under this MOU.

9. NON-DISCRIMINATION

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

9.2 CBO and First 5 Orange County shall furnish any and all information requested by County and shall permit County access, during business hours, to books, records, and accounts directly related to this MOU, to the extent permitted by law, in order to ascertain CBO's and First 5 Orange County's compliance with Paragraph 9 et seq.

9.3 Non-Discrimination in Employment

9.3.1 All solicitations or advertisements for employees placed by or on behalf of CBO and First 5 Orange County shall state that all qualified applicants will receive consideration for employment without regard to race, religious creed, color, national origin, ancestry, physical disability, mental disability, medical condition, genetic information, marital status, sex, gender, gender identity, gender expression, age, sexual orientation, military and veteran status, or any other protected group, in accordance with the requirements of all applicable federal or State laws. Notices describing the provisions of the equal opportunity clause shall be posted in a conspicuous place for employees and job applicants.

9.3.2 CBO and First 5 Orange County shall refer any and all employees desirous of filing a formal discrimination complaint to:

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

9.4 Non-Discrimination in Service Delivery

9.4.1 CBO and First 5 Orange County 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 Code of Federal Regulations (CFR) section 272.6; Title II of the Americans with Disabilities Act of 1990; 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. CBO and First 5 Orange County 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 California Welfare and Institutions Code (WIC) Section

10605, or CGC Sections 11135-11139.5, or any other laws, or the issue may be referred to the appropriate federal agency for further compliance action and enforcement of Subparagraph 9 et seq.

9.4.2 CBO and First 5 Orange County shall provide any and all clients desirous of filing a formal complaint any and all information as appropriate:

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

9.4.2.2 Discrimination Complaint Form

9.4.2.3 Civil Rights Contacts

County Civil Rights Contact

Orange County Social Services Agency

Program Integrity

Attn: Civil Rights Coordinator

P.O. Box 22001

Santa Ana, CA 92702-2001

Telephone: (714) 438-8877

State Civil Rights Contact

California Department of Social Services

Civil Rights Bureau

P.O. Box 944243, M/S 8-16-70

Sacramento, CA 94244-2430

Federal Civil Rights Contact

Office for Civil Rights

U.S. Department of Health and Human Services

90 7th Street, Suite 4-100

San Francisco, CA 94103

Customer Response Center: (800) 368-1019

10. SUBCONTRACTS

10.1 No performance of this MOU or any portion thereof may be subcontracted or otherwise delegated by CBO and First 5 Orange County, in whole or in part, without first obtaining the prior express written consent of County. Any attempt by CBO and First 5 Orange County to subcontract or delegate any performance of this MOU without the prior express written consent of County shall be invalid and shall constitute a material breach of this MOU, and any attempted assignment or delegation in derogation of this paragraph shall be void.

In the event that CBO and/or First 5 Orange County are authorized by County to subcontract, this MOU shall take precedence over the terms of the agreement between CBO and/or First 5 Orange County and subcontractor, and any agreement between CBO and/or First 5 Orange County and a subcontractor shall incorporate by reference the terms of this MOU. CBO and First 5 Orange County shall remain responsible for the performance of this MOU and indemnification of County notwithstanding the County's consent to CBO's and First 5 Orange County'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 CBO and First 5 Orange County and must meet the approval of the County of Orange pursuant to the terms of this MOU.

10.2 Subcontracts of $50,000 or less

CBO and First 5 Orange County shall develop a standard form Purchase Order, subject to prior written approval of County, to be utilized for the purchase of services by CBO and First 5 Orange County when the cumulative total cost of the services to be provided by any organization is anticipated to be $50,000 or less during the term of this MOU. The basis for costs incurred by any such Purchase Order(s) shall be the actual cost of providing services or the usual and customary charges established by the organization(s) providing the services.

10.3 Subcontracts in excess of $50,000

CBO and First 5 Orange County shall follow First 5 Orange County's Board of Commissioners adopted procurement policies for the procurement of subcontracts with any organization in which the total cumulative cost of services provided by any single organization is anticipated to exceed $50,000 during the term of this MOU.

10.4 CBO and First 5 Orange County shall comply with such procurement system in obtaining subcontracts with a total cost in excess of $50,000 during the term of this MOU. In addition, CBO and First 5 Orange County shall obtain County's written consent prior to entering into a subcontract with any organization when the total cumulative cost of services to be provided by that organization is anticipated to exceed $50,000 during the term of this MOU.

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

11. CONFIDENTIALITY

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

11.2 All records and information concerning any and all persons referred to CBO and First 5 Orange County by County or County's designee shall be considered and kept confidential by CBO and First 5 Orange County, CBO and First 5 Orange County's employees, agents, subcontractors, and all other individuals performing services under this MOU. CBO and First 5 Orange County shall require all employees, agents, subcontractors, and all other individuals performing services under this MOU to sign an agreement with CBO and First 5 Orange County before

commencing the provision of any such services, agreeing to maintain confidentiality pursuant to this MOU.

11.3 CBO and First 5 Orange County shall inform all of its employees, agents, subcontractors, and all other individuals performing services under this MOU of this provision and that any person violating the provisions of said California state law may be guilty of a crime.

11.4 CBO and First 5 Orange County agree that any and all subcontracts entered into shall be subject to the confidentiality requirements of this MOU.

11.5 CBO and First 5 Orange County agree 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.

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

11.5.2 CBO and First 5 Orange County 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.

12. PUBLICITY, LITERATURE, ADVERTISEMENTS AND SOCIAL MEDIA

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

12.2 First 5 Orange County owns all rights to the name, logos, and symbols of First 5 Orange County. The use and/or reproduction of First 5 Orange County's name,

logos, or symbols for any purpose, including commercial advertisement, promotional purposes, announcements, displays, or press releases, without First 5 Orange County's prior written consent is expressly prohibited.

12.3 CBO and/or First 5 Orange County may develop and publish information related to this MOU where all of the following conditions are satisfied:

12.3.1 County provides its written approval of the content and publication of the information at least 30 days prior to CBO and/or First 5 Orange County publishing the information, unless a different timeframe for approval is agreed upon by County;

12.3.2 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;

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

12.3.3.1 any commercial product or service; and

12.3.3.2 any product or service provided by CBO and/or First 5 Orange County, unless approved in writing by County; and

12.3.4 If CBO and/or First 5 Orange County uses social media (such as Facebook, Twitter, YouTube or other publicly available social media sites) to publish information related to this MOU, CBO and/or First 5 Orange County shall develop social media policies and procedures and have them available to the County. CBO and First 5 Orange County 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 MOU. The policy is available on the Internet at https://cio.ocgov.com/egovernment-policies.

13. INDEMNIFICATION

13.1 CBO and First 5 Orange County agree to indemnify, defend with counsel approved in writing by County, and hold U.S. Department of Health and Human Services,

the State, County, and their elected and appointed officials, officers, employees, agents, and those special districts and agencies which County's Board of Supervisors acts as the governing Board ('County Indemnitees') harmless from any claims, demands, or liability of any kind or nature, including, but not limited to, personal injury or property damage, arising from or related to the services, products, or other performance provided by CBO and First 5 Orange County pursuant to this MOU. If judgment is entered against CBO and/or First 5 Orange County and County by a court of competent jurisdiction because of the concurrent active negligence of County or County Indemnitees, CBO, First 5 Orange County and County agree that liability will be apportioned as determined by the court. Neither Party shall request a jury apportionment.

13.2 County agrees to indemnify, defend, with counsel approved in writing by First 5 Orange County and approval shall not be unreasonably withheld, and hold First 5 Orange County and their appointed officials, Commissioners, officers, employees, and agents ("First 5 Orange County Indemnitees") harmless from any claims, demands, or liability in the event of a security breach during the transmission of client confidential information from County to First 5 Orange County or CBOs, or arising from or related to the intentional, malicious, negligent acts, errors or omissions of the County of Orange, its officers, employees, or agents pursuant to this MOU. If judgment is entered against County and First 5 Orange County by a court of competent jurisdiction because of the concurrent active negligence of the First 5 Orange County or First 5 Orange County Indemnitees, the County and First 5 Orange County agree that liability will be apportioned as determined by the court. Neither Party shall request a jury apportionment.

13.3 CBO agrees to indemnify, defend with counsel approved in writing by First 5 Orange County, and hold the First 5 Orange 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 CBO pursuant to this MOU.

14. INSURANCE

14.1 Prior to the provision of services under this MOU, CBO and First 5 Orange County agree to carry all required insurance at CBO's and First 5 Orange County's expense, respectively, including all endorsements required herein, necessary to satisfy County that the insurance provisions of this MOU have been complied with. CBO and First 5 Orange County agree to keep such insurance coverage current, provide Certificates of Insurance and endorsements to County during the entire term of this MOU.

14.2 CBO and First 5 Orange County shall ensure that all subcontractors performing work on behalf of CBO and First 5 Orange County pursuant to this MOU shall be covered under CBO's and First 5 Orange County's insurance as an Additional Insured or maintain insurance subject to the same terms and conditions as set forth herein for CBO and First 5 Orange County. CBO and First 5 Orange County shall not allow subcontractors to work if subcontractors have less than the level of coverage required by County from CBO and First 5 Orange County under this MOU. It is the obligation of CBO and First 5 Orange County 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 CBO and First 5 Orange County through the entirety of this MOU for inspection by County representative(s) at any reasonable time.

14.3 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 CBO and First 5 Orange County. If CBO and/or First 5 Orange County are self-insured, CBO and/or First 5 Orange County will indemnify County for any and all claims resulting or arising from CBO's and/or First 5 Orange County's services in accordance with the indemnity provision stated

in this MOU.

14.4 If CBO and First 5 Orange County fail to maintain insurance acceptable to County for the full term of this MOU, County may terminate this MOU.

14.5 Qualified Insurer:

14.5.1 The policy or polices 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).

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

14.5.3 The policy or policies of insurance maintained by CBO and First 5 Orange County shall provide the minimum limits and coverage as set forth below:

| Coverage | Minimum Limits | Responsible Party/ Partner Agency |
|---|---|---|
| Commercial General Liability | $1,000,000 per occurrence<br>$2,000,000 aggregate | CBO and First 5 Orange County |
| Automobile Liability including coverage for owned, non-owned and hired vehicles | $1,000,000 combined single limit each accident | CBO |
| Passenger Vehicles up to four (4) passengers, not including the driver | $1,000,000 combined single limit each accident | |
| Passenger Vehicles up to seven (7) passengers, not including the driver | $2,000,000 combined single limit each accident | |
| Passenger Vehicles up to eight (8) passengers, not including the driver | $5,000,000 combined single limit each accident | |

| | | |
|---|---|---|
| Worker's Compensation | Statutory | CBO and First 5 Orange County |
| Employer's Liability Insurance | $1,000,000 accident or disease | CBO and First 5 Orange County |
| Network Security & Privacy Liability | $1,000,000 per claims-made | CBO and First 5 Orange County |
| Professional Liability Insurance | $1,000,000 per claims-made or occurrence $1,000,000 aggregate | CBO |
| Sexual Misconduct Liability | $1,000,000 per occurrence | CBO |

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

14.6 Required Coverage Forms

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

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

14.7 Required Endorsements

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

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

14.7.1.2 A primary non-contributory endorsement using ISO form CG 20 01 04 13, or a form at least as broad, evidencing that CBO's and First 5 Orange County's insurance is primary and any insurance or self-insurance maintained by the County shall be excess and non-contributory.

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

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

14.7.2.2 A primary and non-contributory endorsement evidencing that the CBO's and First 5 Orange County's insurance is primary and any insurance or self-insurance maintained by the County shall be excess and non-contributing.

14.7.3 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.

14.8 All insurance policies required by this MOU 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.

14.9 CBO and First 5 Orange County shall provide 30 days prior written notice to 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 MOU, upon which the County may suspend or terminate this MOU.

14.10 If CBO's and First 5 Orange County's Professional Liability or Network Security & Privacy Liability policy are "Claims-Made" policies, CBO and First 5 Orange County shall agree to the following:

14.10.1 The retroactive date must be shown and must be before the date of the MOU or the beginning of the MOU services.

14.10.2 Insurance must be maintained, and evidence of insurance must be provided for at least three years after expiration or earlier termination of MOU services.

14.10.3 If coverage is canceled or non-renewed, and not replaced with another claims-made policy form with a retroactive date prior to the effective date of the MOU services, CBO and First 5 Orange County must purchase an extended reporting period for a minimum of three years after expiration of earlier termination of the MOU.

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

14.12 Insurance certificates should be forwarded to County at the address indicated in Paragraph 21 of this MOU.

14.13 Failure of CBO and/or First 5 Orange County to provide the insurance certificates and endorsements within seven days of notification by CEO/County Procurement Office or County, will result in a breach of this MOU.

14.14 County expressly retains the right to require CBO and First 5 Orange County to increase or decrease insurance of any of the above insurance types throughout the term of this MOU. Any increase or decrease in insurance will be as deemed by County of Orange Risk Manager as appropriate to adequately protect County.

14.15 County shall notify CBO and First 5 Orange County in writing of changes in the

insurance requirements. If CBO and First 5 Orange County do not provide acceptable Certificates of Insurance and endorsements to County incorporating such changes within 30 days of receipt of such notice, this MOU may be in breach without further notice to CBO and/or First 5 Orange County, and County shall be entitled to all legal remedies.

14.16 The procuring of such required policy or policies of insurance shall not be construed to limit CBO's and First 5 Orange County's liability hereunder nor to fulfill the indemnification provisions and requirements of this MOU, nor act in any way to reduce the policy coverage and limits available from the insurer.

15. SECURITY

CBO and First 5 Orange County shall abide by the requirements in Attachments A and B of this MOU, which are hereby incorporated by reference and attached hereto.

16. NOTIFICATION OF INCIDENTS, CLAIMS, OR SUITS

CBO and First 5 Orange County shall report to County, in writing within 24 hours of occurrence, the following:

16.1 Any accident or incident relating to services performed under this MOU that involves injury or property damage which may result in the filing of a claim or lawsuit against CBO, First 5 Orange County and/or County.

16.2 Any third party claim or lawsuit filed against CBO and/or First 5 Orange County arising from or relating to services performed by CBO and/or First 5 Orange County under this MOU.

16.3 Any injury to an employee of CBO and/or First 5 Orange County that occurs on County property.

16.4 Any loss, disappearance, destruction, misuse, or theft of any kind whatsoever of County property, monies, or securities entrusted to CBO and/or First 5 Orange County under the term of this MOU.

17. RECORDS

17.1 Client Records

17.1.1 CBO and First 5 Orange County shall prepare and maintain accurate and complete records of clients served and dates and type of services provided under the terms of this MOU in a form acceptable to County.

17.1.2 CBO and First 5 Orange County shall keep all County data provided to CBO and First 5 Orange County during the term(s) of this MOU for a minimum of five years from the date of final payment under this MOU or until all pending County, State, and federal audits are completed, whichever is later. These records shall be stored in Orange County, unless CBO and/or First 5 Orange County 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 MOU, CBO and First 5 Orange County shall relinquish control with respect to County data to County in accordance with Subparagraph 25.2 of this MOU.

17.2 Public Records

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

18. PERSONNEL DISCLOSURE

18.1 This Paragraph 18 applies to all of CBO's and First 5 Orange County's personnel providing services through this MOU, paid and unpaid (herein referred to as "Personnel").

18.2 CBO and First 5 Orange County 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:

18.2.1 Names and dates of birth of all Personnel by title, whose direct services are required to provide the programs described herein;

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

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

18.2.4 The language skill, if applicable, for all Personnel.

18.3 Where authorized by law, and in a manner consistent with California Government Code Section 12952, CBO and First 5 Orange County 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 MOU.

18.4 Where authorized by law, CBO and First 5 Orange County 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 MOU: U.S. Department of Justice National Sex Offender Website (www.nsopw.gov) and Megan's Law Sex Offender Registry (www.meganslaw.ca.gov).

18.5 Where authorized by law, CBO and First 5 Orange County 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 MOU. 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 MOU.

18.6 CBO and First 5 Orange County shall ensure that clearances and background checks described in Subparagraphs 18.4 and 18.5 are completed prior to CBO's and First 5 Orange County's Personnel providing services under this MOU.

18.7 In the event a record is revealed through the processes described in Subparagraphs 18.4 and 18.5, County will be available to consult with CBO and First 5 Orange County on appropriateness of Personnel providing services through this MOU.

18.8 CBO and First 5 Orange County warrant that all Personnel assigned by CBO and First 5 Orange County to provide services under this MOU 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 MOU. CBO and First 5 Orange County shall maintain records of background investigations and reference checks undertaken and coordinated by CBO and First 5 Orange County for Personnel assigned to provide services under this MOU, for a minimum of five years from the date of final payment under this MOU, or until all pending County, State, and federal audits are completed, whichever is later, in compliance with all applicable laws.

18.9 CBO and First 5 Orange County 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 MOU, when such information becomes known to CBO and First 5 Orange County. County, at its sole discretion, may determine whether such Personnel may continue to provide services under this MOU and shall provide notice of such determination to CBO and First 5 Orange County in writing. CBO's and/or First 5 Orange County's failure to comply with County's decision shall be deemed a material breach of this MOU.

18.10 County has the right to approve or disapprove all of CBO's and First 5 Orange County's Personnel performing work hereunder, and any proposed changes in CBO's and First 5 Orange County's Personnel.

18.11 County shall have the right to require CBO and First 5 Orange County to remove any Personnel from the performance of services under this MOU. At the request of County, CBO and First 5 Orange County shall immediately replace said Personnel.

18.12 CBO and First 5 Orange County shall notify County immediately when Personnel is terminated for cause from working on this MOU.

18.13 Disqualification, if any, of CBO and First 5 Orange County Personnel, pursuant to this Paragraph 18, shall not relieve CBO and First 5 Orange County of their obligation to complete all work in accordance with the terms and conditions of this MOU.

19. CHILD AND DEPENDENT ADULT/ELDER ABUSE REPORTING

CBO and First 5 Orange County shall establish a procedure acceptable to County to ensure that all employees, agents, subcontractors, and all other individuals performing services under this MOU 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 WIC Section 15610.07 to one of the agencies specified in WIC Section 15630. CBO and First 5 Orange County shall require such employees, agents, subcontractors, and all other individuals performing services under this MOU 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.

20. NOTICE TO EMPLOYEES REGARDING THE SAFELY SURRENDERED BABY LAW

CBO and First 5 Orange County shall notify and provide to its employees, a fact sheet regarding the Safely Surrendered Baby Law, its implementation in Orange County, and where and how to safely surrender a baby. The fact sheet is available on the Internet at www.babysafe.ca.gov for printing purposes. The information shall be posted in all reception areas where clients are served.

21. NOTICES

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

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

Asian American Senior Citizens Service Center, Inc.
Attn: Executive Director
850 N. Birch Street
Santa Ana, CA 92701

First 5 Orange County
Attn: President/Chief Executive Officer
1505 East 17th Street
Santa Ana, CA 92705

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

22. RESOLUTION OF CONFLICTS

For resolution of conflicts between County, CBO, and First 5 Orange County in regards to the provisions of this MOU, the following shall apply:

Step 1: Conference between the County Program Manager and the CBO's and First 5 Orange County's Program Coordinator(s).

Step 2: Conference between the County Deputy Director or designee, and the CBO's and First 5 Orange County's Program Director(s).

Step 3: Conference between the County Children and Family Services Division Director or designee and the CBO's and First 5 Orange County's Executive Director(s) or designee.

Nothing in this Paragraph 22 limits the rights of the Parties under Paragraph 25.

23. CONFLICT OF INTEREST

23.1 CBO and First 5 Orange County shall exercise reasonable care and diligence to prevent any actions or conditions that could result in a conflict with the best interests of the County. This obligation shall apply to CBO and First 5 Orange County and the CBO's and First 5 Orange County's employees, agents, and subcontractors associated with accomplishing work and services hereunder. CBO's and First 5 Orange County'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 the County.

23.2 CBO and First 5 Orange County shall notify County, in writing, of any potential or actual conflicts of interest between CBO and/or First 5 Orange County and County that may arise prior to, or during the period of, MOU performance, including, but not limited to, whether any known County public officer's child is an officer or director of, or has an ownership interest of 10 percent or more in, CBO and/or First 5 Orange County. While CBO and First 5 Orange County will be required to provide this information without prompting from County any time there is a change regarding conflict of interest, CBO and First 5 Orange County must also provide an update to County upon request by County.

23.3 County of Orange Board of Supervisors policy prohibits its employees from engaging in activities involving a conflict of interest. Unless otherwise authorized by County, CBO and First 5 Orange County shall not, during the period of this MOU, employ any County employee for any purpose.

24. POLITICAL ACTIVITY

The Parties agree 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.

25. TERMINATION

25.1 County may terminate this MOU 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 limited to, any breach of this MOU, any partial misrepresentation whether negligent or willful, fraud on the part of CBO and/or First 5 Orange County, discontinuance of the services for reasons within CBO's and/or First 5 Orange County's reasonable control, and repeated or continued violations of County ordinances unrelated to performance under this MOU that, in the reasonable opinion of County, indicate a willful or reckless disregard for County laws and regulations. Except for the indemnity provisions, exercise by County of the right to terminate this MOU shall relieve County of all further obligations under this MOU.

25.2 For 90 calendar days prior to the expiration date of this MOU, or upon notice of termination of this MOU ("Transition Period"), CBO and First 5 Orange County agree 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, services and data access shall continue to be made available to County without alteration. CBO and First 5 Orange County also shall assist County in extracting and/or transitioning all data in the format determined by County.

25.3 In the event of termination of this MOU, cessation of business by CBO and/or First 5 Orange County, or any other event preventing CBO and First 5 Orange County from continuing to provide services, CBO and First 5 Orange County 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 MOU.

25.4 The obligations under this MOU utilize County resources, for which funding, or portions of funding, may be contingent upon the State and/or federal budget; receipt of funds from and/or obligation of funds by the State and/or Federal Government; and inclusion of sufficient funding for the services hereunder in the budget approved by the County's Board of Supervisors for each fiscal year covered by this MOU. If such approval, funding, or appropriations are not forthcoming, or are otherwise limited, County may terminate, reduce, or modify this MOU without penalty.

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

26. SIGNATURE IN COUNTERPARTS

The Parties agree that separate copies of this MOU may be signed by each of the Parties, and this MOU will have the same force and effect as if the original had been signed by all Parties. CBO and First 5 Orange County represent and warrant that the person executing this MOU on behalf of and for CBO and First 5 Orange County is an authorized agent who has actual authority to bind CBO and First 5 Orange County to each and every term, condition and obligation of this MOU and that all requirements of CBO and First 5 Orange County have been fulfilled to provide such actual authority.

27. GENERAL PROVISIONS

27.1 Nothing herein contained shall be construed as creating the relationship of employer and employee, or principal and agent, between County and any participant participating in this program, or any of CBO and First 5 Orange County's agents or employees.

27.2 This MOU, with its Attachments and Exhibit incorporated herein by reference

represents the entire understanding of the Parties with respect to the subject matter. No change, modification, extension, termination or waiver of this MOU, or any of the understandings herein contained, shall be valid unless made in writing and signed by duly authorized representatives of the Parties hereto.

27.3 This MOU 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. In the event of any legal action to enforce or interpret this MOU, 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.

27.4 CBO and First 5 Orange County warrant that it and its Personnel, described in Paragraph 18 of this MOU, 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, County of Orange, and all other appropriate governmental agencies to perform the services described in this MOU, and agrees to maintain, and require its Personnel to maintain, these licenses and permits in effect for the duration of this MOU. CBO and First 5 Orange County must notify County within one business day of any change in license or permit status (e.g., becoming expired, inactive, etc.).

27.5 In the performance of this MOU, CBO and First 5 Orange County shall comply with 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.

27.6 In the performance of this MOU, CBO and First 5 Orange County 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.

27.7 The various headings, numbers, and organization herein are for the purpose of convenience only and shall not limit or otherwise affect the meaning of this MOU.

WHEREFORE, the Parties hereto have executed the Memorandum of Understanding in the County of Orange, California.

Signed by:
By: Kimberly Goll 2651BE09D88E4C6... Dated: 3/16/2026 | 10:33:01 AM PDT

Kimberly Goll

President/Chief Executive Officer

First 5 Orange County

DocuSigned by:
By: Jennifer S. Wang 64349FD1F41445A... Dated: 3/16/2026 | 10:32:25 AM PDT

Jennifer S. Wang

Executive Director

Asian American Senior Citizens Service Center, Inc.

COUNTY OF ORANGE

By:_____ Dated:_____

Deputy Procurement Agent

County of Orange, Social Services Agency

Approved As To Form

SSA Counsel

County of Orange, California

By:_____ Dated:_____

Deputy County Counsel

WHEREFORE, the Parties hereto have executed the Memorandum of Understanding in the County of Orange, California.

By:_____ Dated:_____

Kimberly Goll

President/Chief Executive Officer

First 5 Orange County

By:_____ Dated:_____

<<Name>>

<<Title>>

<<CBO>>

COUNTY OF ORANGE

By:_____ Dated:_____

Deputy Procurement Agent

County of Orange, Social Services Agency

Approved As To Form

SSA Counsel

County of Orange, California

By: DocuSigned by: Carolyn S. Frost D3AB98D76D0B425... Dated: 3/4/2026 | 1:23:08 PM PST

Deputy County Counsel

# ATTACHMENT A

## COUNTY OF ORANGE INFORMATION TECHNOLOGY SECURITY PROVISIONS

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

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

A. Ensure the confidentiality, integrity, and availability of all County data and any other confidential information that the Contractor receives, stores, maintains, processes, transmits, or otherwise accesses in connection with the provision of the contracted services,

B. Protect against any threats or hazards to the security or integrity of County data, systems, or other confidential information,

C. Protect against unauthorized access, use, or disclosure of personal or County confidential information,

D. Maintain reasonable procedures to prevent, detect, respond, and provide notification to the County regarding any internal or external security breaches,

E. Ensure the return or appropriate disposal of personal information or other confidential information upon contract conclusion (or per retention standards set forth in the contract), and

F. Ensure that any subcontractor(s)/agent(s) that receives, stores, maintains, processes, transmits, or otherwise accesses County data and/or system(s) is in compliance with statements and the provisions of statements and services herein.

**2. County of Orange Information Technology Security Provisions Document:**

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

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

Contractor shall use industry best practices and methods with regard to confidentiality, integrity, availability, and the prevention, detection, response, and elimination of threat, by all

appropriate means, of fraud, abuse, and other inappropriate or unauthorized access to County data and/or system(s) accessed in the performance of Services under this Contract.

**3. Contractor's Information Security Program:**

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

**4. Information Access:**

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

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

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

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

**5. Data Security Requirements:**

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

B. Contractor also shall provide technical and organizational safeguards against accidental, unlawful, or unauthorized access or use, destruction, loss, alteration, disclosure, transfer, commingling, or processing of such information that ensure a level of security appropriate to the risks presented by the processing of County Data, Contractor personnel and/or subcontractor personnel and affiliates approved by County to perform work under this Contract may use or disclose County personal and confidential information only as permitted in this Contract. Any other use or disclosure requires express approval in writing by the County of Orange. No Contractor personnel and/or subcontractor personnel or affiliate shall duplicate, disseminate, market, sell, or disclose County personal and confidential information except as allowed in this Contract. Contractor personnel and/or subcontractor personnel or affiliate who access, disclose, market, sell, or use County personal and confidential information in a manner or for a purpose not authorized by this Contract may be subject to civil and criminal sanctions contained in applicable federal and state statutes.

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

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

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

**6. Enhanced Security Measures:**

County may, in its discretion, designate certain areas, facilities, or solution systems as ones that require a higher level of security and access control. County shall notify Contractor in writing reasonably in advance of any such designation becoming effective. Any such notice shall set forth, in reasonable detail, the enhanced security or access-control procedures, measures, or requirements that Contractor shall be required to implement and enforce, as well as the date on which such procedures and measures shall take effect. Contractor shall and shall

cause Contractor personnel and subcontractors to fully comply with and abide by all such enhanced security and access measures and procedures as of such date.

**7. General Security Standards:**

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

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

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

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

**8. Security Failures:**

Any failure by the Contractor to meet the requirements of this Contract with respect to the security of County data, including any related backup, disaster recovery, or other policies, practices or procedures, and any breach or violation by Contractor or its subcontractors or affiliates, or their employees or agents, of any of the foregoing, shall be deemed a material breach of this Contract and may result in termination and reimbursement to County of any fees prepaid by County prorated to the date of such termination. The remedy provided in this paragraph shall not be exclusive and is in addition to any other rights and remedies provided by law or under the Contract.

**9. Security Breach Notification:**

A. In the event Contractor becomes aware of any act, error or omission, negligence, misconduct, or security incident including unsecure or improper data disposal, theft, loss, unauthorized use and disclosure or access, that compromises or is suspected to compromise the security, availability, confidentiality, and/or integrity of County data or the physical, technical, administrative, or organizational safeguards required under this Contract that relate to the security, availability, confidentiality, and/or integrity of County data, Contractor shall, at its own expense,

1. Immediately (or within 24 hours of potential or suspected breach), notify the County's Chief Information Security Officer and County Privacy Officer of such occurrence;
2. Perform a root cause analysis of the actual, potential, or suspected breach;
3. Provide a remediation plan that is acceptable to County within 30 days of verified breach, to address the occurrence of the breach and prevent any further incidents;
4. Conduct a forensic investigation to determine what systems, data, and information have been affected by such event; and
5. Cooperate with County and any law enforcement or regulatory officials investigating such occurrence, including but not limited to making available all relevant records, forensics, investigative evidence, logs, files, data reporting, and other materials required to comply with applicable law or as otherwise required by County and/or any law enforcement or regulatory officials, and
6. Perform or take any other actions required to comply with applicable law as a result of the occurrence (at the direction of County).

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

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

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

Notification shall be sent to:

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

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

**10. Security Audits:**

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

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

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

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

**11. <u>Business Continuity and Disaster Recovery (BCDR):</u>**

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

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

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

# ATTACHMENT B - 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@$$S. This is ok: P@$S$)

      vii. COMPLEX PASSWORD EXAMPLE: P@$SWoRd13

viii. Passphrases example: The$kyIsBlue2day

ix. Passwords cannot contain the user's full name or network login.

c. Passwords shall have a minimum length of twelve (12) characters.

d. Passwords shall not be reused for twelve (12) iterations.

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

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

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

h. No user shall give his or her password to another person under any circumstances. Workforce members who suspect that their password has become known by another person shall change their password immediately and report their suspicion to management.

i. Users who have lost or forgotten their passwords shall make any password reset requests themselves without using a proxy (e.g., another County employee) unless approved by management. Prior to processing password change requests, the requester shall be authenticated to the user account in question. (e.g., Verification with user's supervisor or the use of passphrases can be used for this authentication process.) New passwords shall be provided directly and only to the user in question.

j. When technologically feasible, a new or reset password shall be set to expire on its initial use at log on so that the user is required to change the provided password to one known only to them.

k. All passwords are to be treated as sensitive information.

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

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

C. **Inactivity Timeout and Restricted Connection Times**

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

2. Automated screen lockouts shall be used wherever possible using a set time increment (e.g., 15 minutes of non-activity). In situations where it is not possible to automate a lockout, operational procedures shall be implemented to instruct users to lock the terminal

or equipment so that unauthorized individuals cannot make use of the system. Once logged on, workforce members shall not leave their computer unattended or available for someone else to use.

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

D. **Account Monitoring**

1. Access to a County network and its resources shall be strictly controlled, managed, and reviewed to ensure only authorized users gain access based on the privileges granted. (e.g., Kiosks provide physical and public access to County networks. These shall be secured to ensure County resources are not accessed by unauthorized users.)
2. The control mechanisms for all types of access to County IT resources by contractors, customers or vendors are to be documented.
3. Monitor account usage to determine dormant accounts that have not been used for a given period, such as 45 days, notifying the user or user's manager of the dormancy.
4. After a longer period, such as 60 days, the account shall be disabled by the system when the technology is feasible or available.
5. On a periodic basis, such as quarterly or at least annually, departments shall require that managers match active employees and contractors with each account belonging to their managed staff. Security or system administrators shall then determine whether to disable accounts that are not assigned to active employees or contractors.

E. **Administrative Privileges**

1. Systems Administrators shall use separate administrative accounts, which are different from their end user account (required to have an individual end user account), to conduct system administration tasks.
2. Administrative accounts shall only be granted to individuals who have a job requirement to conduct systems administration tasks.
3. Administrative accounts shall be requested in writing and must be approved by the Department Head or designated representative using the Security Review and Approval Process.
4. Systems Administrator accounts that access County enterprise-wide systems or have enterprise-wide impact shall be approved by the CISO using the Security Review and Approval Process.
5. Systems Administrators shall use separate administrative accounts to manage Mobile Device Management (MDM) platforms but may use the local user's credentials when configuring a mobile phone or tablet device.
6. All passwords for privileged system-level accounts (e.g., root, enable, OS admin, application administration accounts, etc.) shall comply with Controls Management B.7.

F. **Remote Access**

1. Departments and/or contractors shall take appropriate steps, including the implementation of appropriate encryption, user authentication, and virus protection measures, to mitigate security risks associated with allowing users to use remote access or mobile computing methods to access County information systems.
2. Remote access privileges shall be granted to County workforce members only for legitimate business needs and with the specific approval of department management.
3. All remote access implementations that utilize the County's trusted network environment and that have not been previously deployed within the County shall be submitted to and reviewed by the County. A memorandum of understanding (MOU) shall be utilized for this submittal and review process. This is required for any Suppliers utilizing remote access to conduct maintenance.
4. Remote sessions shall be terminated after 15 minutes of inactivity requiring the user to authenticate again to access County resources.
5. All remote access infrastructures shall include the capability to monitor and record a detailed audit trail of each remote access attempt.
6. All users of County networks and computer systems are prohibited from connecting and/or activating unauthorized dial-up or broadband modems on workstations, laptops, or other computing devices that are simultaneously connected to any County network.
7. Periodic assessments shall be performed to identify unauthorized remote connections. Results shall be used to address any vulnerabilities and prioritized according to criticality.
8. Users granted remote access to County IT infrastructure shall follow all additional policies, guidelines and standards related to authentication and authorization as if they were connected locally. For example, this applies when mapping to shared network drives.
9. Users attempting to use external remote access shall utilize a County-approved multi-factor authentication process.
10. All remote access implementations that involve non-County infrastructures shall be reviewed and approved by both the department and the County. This approval shall be received prior to the start of such implementation.
11. Remote access privileges to County IT resources shall not be given to contractors and customers unless department management determines that these individuals or organizations have a legitimate business need for such access. If such access is granted, it shall be limited to those privileges and conditions required for the performance of the specified work.

G. **Wireless Access**

1. Departments and/or contractors shall take appropriate steps, including the implementation of appropriate encryption, user authentication, device authentication and

malware protection measures, to mitigate risks to the security of County data and information systems associated with the use of wireless network access technologies.

2. Only wireless systems that have been evaluated for security by both department management and the County shall be approved for connectivity to County networks.
3. County data that is transmitted over any wireless network shall be protected in accordance with the sensitivity of the information.
4. All access to County networks or resources via unapproved wireless communication technologies is prohibited. This includes wireless systems that may be brought into County facilities by visitors or guests. Employees, contractors, vendors and customers are prohibited from connecting and/or activating wireless connections on any computing device that are simultaneously connected to any County network, either locally or remotely.
5. Each department and/or contractor shall make a regular, routine effort to ensure that unauthorized wireless networks, access points, and/or modems are not installed or configured within its IT environments. Any unauthorized connections described above shall be disabled immediately.

H. **System and Network Operations Management**

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

I. **System Monitoring and Logging**

1. Systems operational staff shall maintain appropriate log(s) of activities, exceptions and information security events involving County information systems and services.
2. Each department and/or contractor shall maintain a log of all faults involving County information systems and services.
3. Logs shall be protected from unauthorized access or modifications wherever they reside.
4. The clocks of all relevant information processing systems and attributable logs shall be synchronized with an agreed upon accurate time source such as an established Network Time Protocol (NTP) service.
5. Auditing and logging of user activity shall be implemented on all critical County systems that support user access capabilities.

6. Periodic log reviews of user access and privileges shall be performed in order to monitor access of sensitive information.

J. **Malware Defenses**

1. Departments shall implement endpoint security on computing devices connected to the County network. Endpoint security may include one or more of the following software: anti-virus, 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.

**EXHIBIT A**

MEMBER CERTIFICATION OF
NEIGHBORHOOD RESOURCE NETWORK MULTIDISCIPLINARY TEAM

To: Orange County Social Services Agency
Children and Family Services
Attention: NRN Contract Administrator
500 N. State College Blvd., Suite 100
Orange, CA 92868

_____ hereby designates the following person as a member of (Commission/CBO) the Orange County Social Services Agency (SSA) NRN multidisciplinary personnel team (MDT):

Name: _____
Title: _____
Agency: _____
Address: _____
_____
Phone: _____

The above Commission/CBO/MDT member hereby certifies that it has provided training to the above-designated person as required by Subparagraph 6.3.2, 6.3.3, and 7.6 of the Memorandum of Understanding (MOU) between SSA and Commission/CBOs/MDT member to establish a MDT for NRN Services (MA-063-26010592), and certifies that its designee is qualified to provide a broad range of services related to child abuse or neglect.

_____ Dated: _____
Commission/CBO Member Signature

_____ Title: _____
Print Name

I hereby certify that I have received the required training and am qualified to provide a broad range of services related to child abuse and neglect, and that I, understand the scope and purpose of the MDT and agree to keep all information confidential.

_____ Dated: _____
MDT Member Signature

_____
Print Name