MEMORANDUM OF UNDERSTANDING
FOR THE PROVISION OF
SYSTEM OF CARE FOR CHILDREN, YOUTH AND FAMILIES IN ORANGE COUNTY

This Memorandum of Understanding (MOU) is entered into by and between the County of Orange, acting through its Social Services Agency (SSA), Health Care Agency (HCA), and Probation Department (Probation), hereinafter referred to as "County;" the County of Orange, Orange County Superintendent of Schools, also known as the Orange County Department of Education, hereinafter referred to as "OCDE;" the Regional Center of Orange County, hereinafter referred to as "RCOC;" and the Children and Families Commission of Orange County, also known as First 5 Orange County, hereinafter referred to as "First 5 Orange County." This MOU establishes the expectations for the design, delivery and management of services to children and youth in Orange County, including, but not limited to, children and youth in foster care, non-minor dependents (NMDs), and children, youth, and families who have experienced severe trauma or are at risk of future trauma. These individuals, referred to as "Target Population," as defined under Paragraph 4 of this MOU, may be involved in, or at risk of being involved in, the child welfare and/or probation systems in Orange County. All services developed or coordinated pursuant to this MOU shall be delivered within a Trauma-Informed System of Care.

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

1. This MOU is established in a collaborative effort, in accordance with Welfare and Institutions Code (WIC) §16521.6 (State of California Assembly Bill (AB) 2083, effective September 27, 2018) to ensure that coordinated, timely, and trauma-informed services are provided to children and youth in foster care who have experienced severe trauma.
2. Consistent with All County Letter (ACL) 19-226, this MOU represents the aligned and shared roles and responsibilities of the local agencies serving children and youth in foster care, and that while AB 2083 focuses on children and youth in foster care who have experienced severe trauma, this MOU also reflects a priority to build a locally-governed interagency or interdepartmental model on behalf of all children and youth across California that have similar needs, that interact with and are served by multiple agencies by expanding the "Target Population" to include children, youth, and families outside of the foster care system as outlined in this MOU.
3. This MOU recognizes the Parties as local system partners involved in the coordination and delivery of public programs and services that support caregivers and providers in meeting the educational, developmental, physical, emotional, and behavioral health needs of children and youth in Orange County, including, but not limited to, children and youth in foster care, NMDs, and children, youth and families who have experienced severe trauma

or are at risk of future trauma, any of whom may be involved in or at risk of being involved in the child welfare and/or probation systems in Orange County.

4. This MOU provides a framework that will guide the operations and the activities, decisions, and direction of each of the local system partners that serve such children, youth and families.
5. This MOU sets forth the procedures authorized by the SSA Child Welfare Director, HCA Deputy Agency Director, Chief Probation Officer, OCDE Administrator, RCOC Executive Director, and First 5 Orange County Chief Executive Officer for their respective employees to follow in the provision of these services.
6. This MOU establishes that all Parties are subject to the information and data sharing provisions contained herein for all information and data shared by a Party under this MOU. Notwithstanding the foregoing, only HCA and SSA shall disclose and receive data between themselves regarding mutual clients participating in HCA Behavioral Health Services and SSA Child Welfare Services, and are bound by the requirements set forth in Attachment B. Probation, OCDE, RCOC, and First 5 Orange County are not bound by, nor subject to, Attachment B.
7. This MOU establishes that SSA, HCA, Probation, OCDE, and First 5 Orange County are the only Parties bound by the requirements set forth in Attachments C and D. RCOC is not bound by, nor subject to, Attachments C and D.
8. This is a nonfinancial MOU, and each Party shall be responsible for its own costs.
9. The Parties mutually agree to the following terms and conditions:

TABLE OF CONTENTS

1. TERM

The term of this MOU shall commence on October 1, 2026, and end on September 30, 2031, unless earlier terminated pursuant to the provisions of Paragraph 19 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. MISSION, PURPOSE, GOALS AND PRINCIPLES

2.1 Mission

2.1.1 The Parties to the MOU shall collaboratively promote alignment of public programs for the Target Population to provide trauma-informed services in an integrated, comprehensive, culturally responsive, and evidence-based/best practice manner.

2.1.2 The Parties to the MOU commit to improving the experience of the Target Population navigating public-serving agencies through county-level collaborations and partnerships that manage or oversee the delivery of services to the Target Population who are impacted by or at risk of being impacted by the child welfare and probation systems in Orange County.

2.1.3 Nothing in this MOU shall be construed to require any Party to directly provide services beyond its statutory authority, funding or program capacity. This MOU is intended to facilitate coordination, planning and alignment of existing services and any future services developed within each Party's lawful and funded capacity.

2.2 Purpose

2.2.1 This MOU sets forth the roles and responsibilities of the Parties that serve the Target Population.

2.2.2 This MOU establishes the Parties as a coordinating council and planning body responsible for developing programs and policies that provide coordinated, integrated, and effective trauma-informed services for the Target Population. The Parties will serve as a coordinating body without superseding the authority of any individual Party.

2.2.3 The Parties to the MOU agree that consistent interdepartmental and interagency leadership is essential to successful collaboration on behalf of the Target Population.

2.3 Goals

2.3.1 Develop a coordinated, timely, and Trauma-Informed System of Care for the Target Population.

2.3.2 Address systemic barriers to the provision of interdepartmental and interagency services.

2.3.3 Align service planning and leverage existing processes and structures within and across departments and agencies to provide a comprehensive array of integrated public community-based services, supports, and placements.

2.3.4 Strengthen and continue to formalize the administrative Interagency Leadership Team (ILT) to support cross-system coordination and alignment to the interrelated child welfare, juvenile justice, education, developmental, and children's behavioral health services in Orange County.

2.3.4.1 The Parties do not delegate their legal authority with respect to any core function or power of their agency, office, department, or position.

2.3.4.2 The Parties affirm that nothing in this MOU is intended to conflict with or override any applicable agencywide policies, rules, or agreements.

2.3.4.3 The Parties fully support the structure and processes set forth in this MOU, intended to provide a framework that will guide their agency and employee operations, activities, and decisions involving the Target Population.

2.3.4.4 The ILT shall not have decision-making authority over any Party, including any Party's statutory, fiscal or programmatic responsibilities.

2.4 Principles

2.4.1 Promote and support coordination of services within the System of Care that are trauma-informed, outcome-focused, family-centered, strength-based, culturally informed, and comprehensive. Services coordinated under this MOU will be integrated through a single service plan, to the extent possible, to support the Target Population in developing and leveraging their unique resources and natural supports to overcome challenges.

2.4.2 Identify, develop, and maintain public community-based service systems which can intervene early to respond to and/or prevent challenges experienced by the Target Population.

2.4.3 Promote and support coordination of services to the Target Population in community-based settings that are least restrictive and that minimize stigma.

2.4.4 Identify, develop, and monitor coordinated policies, procedures, resources,

and implementation practices for the benefit of the Target Population.

2.4.5 Adopt confidentiality standards for data sharing as consistent with and authorized by law, including the following:

2.4.5.1 SSA: WIC §§827 through 832, §10850, and §18986.46, 34 Code of Federal Regulations (CFR) 99, Local Rule 903.1 – Exchange of Confidential Information of Orange County Superior Court, and California Rule of Court §5.552 – Confidentiality of Records.

2.4.5.2 HCA: Federal and State privacy and security laws including, without limitation, Health Insurance Portability and Accountability Act of 1996 (HIPAA), the Health Information Technology for Economic and Clinical Health Act (HITECH), Confidentiality of Substance Use Disorder Patient Records (42 CFR Part 2), the California Confidentiality of Medical Information Act (CMIA) (see Civil Code 56 et seq.), Local Rule 903.1 – Exchange of Confidential Information of Orange County Superior Court (if/when HCA is participating in juvenile court matters), and Lanterman-Petris-Short Act (CA WIC §5328 -5330).

2.4.5.3 Probation: Local Rule 903.1 – Exchange of Confidential Information of Orange County Superior Court, WIC §§827 through 832, and California Rule of Court §5.552 – Confidentiality of Records.

2.4.5.4 RCOC: Federal and State privacy laws including, without limitation, HIPAA and the Lanterman Developmental Disabilities Services Act (WIC §4500 et seq.), and Local Rule 903.1 – Exchange of Confidential Information of Orange County Superior Court.

2.4.5.5 OCDE: Family and Educational Rights and Privacy Act (FERPA), as amended (20 U.S.C. §1232g; 34 CFR Part 99), the California Information Practices Act (California Civil Code §1798 et seq.), California Education Code §49060 et seq. (Chapter 6.5, Pupil Records), Student Online Personal Information Protection Act (SOPIPA), Article 1, Section 1 of the California Constitution, Local Rule 903.1 – Exchange of Confidential Information of Orange County Superior Court, and all other applicable federal and State laws and regulations that safeguard education records, privacy, and confidentiality.

2.4.6 Provide ongoing support and guidance to each Party and its staff in providing services and resources for the Target Population consistent with the mission, purpose, goals, and principles of this MOU.

2.4.7 Identify and address barriers to cost sharing and promote use of creative fiscal strategies that responsibly leverage available financial resources in order to provide the Target Population with timely access to an array of quality services.

2.4.8 Incorporate the voices, experiences, and wisdom of the Target Population and caregivers/families into the collaborations and partnerships captured by this MOU.

2.4.9 Ensure the appropriate utilization of treatment and rehabilitation services for the Target Population in conjunction with appropriate court supervision, when applicable, while considering the safety of the community and public-at-large.

2.4.10 Promote and maintain quality services that are cost-effective, evidence-based, and appropriate by evaluating the use of shared service authorization/re-authorization processes and outcomes evaluation, as permitted by law.

2.4.11 Promote coordinated data collection, tracking, and exchange among the Parties, as permitted by law, in a manner that supports consistent and accurate performance measurement.

2.4.12 Prioritize the sharing of information between the Parties, as authorized by law, such that delays in service delivery are minimized.

2.4.13 Promote ongoing communication and engagement with tribal partners in accordance with Attachment A of this MOU (Tribal Consultation Policy).

3. DEFINITIONS

3.1 Child and Family Team (CFT): Per WIC §16501, a group of individuals who are convened by the placing agency and who are engaged through a variety of team-based processes to identify the strengths and needs of the child or NMD and family, and to help achieve positive outcomes for safety, permanency, and well-being.

3.2 Continuum of Care Reform (CCR):

3.2.1 A body of existing and new reforms to California's child welfare services program that provides the statutory and policy framework to ensure that services and support for the Target Population are tailored toward the ultimate goal of maintaining stable permanent families.

3.2.2 Designed to meet the individualized needs of the Target Population in foster care who have experienced trauma, abuse and/or neglect, and provide meaningful supports for the families that care for them.

3.2.3 The goal is to improve the child welfare system through use of

comprehensive child assessments; increased utilization of home-based family care; provision of services and support for home-based family care; reduced reliance on congregate care placement settings; and creation of faster paths to permanency for youth involved in the child welfare and juvenile justice systems.

3.3 Child and Adolescent Needs and Strengths (CANS) Tool: A multi-purpose assessment tool used by the CFT, collaboratively administered by HCA and SSA, to inform decision-making and to monitor the outcome(s) of services. The CANS tool can help guide conversations among CFT members to assess the well-being of children and youth, identify trauma indicators, identify a range of social and behavioral strengths and healthcare needs, inform and support care and service coordination, aid in case planning activities, and inform placement decisions.

3.4 Every Student Succeeds Act (ESSA): The primary federal K-12 education law, focusing on providing high-quality education and reducing federal overreach by transferring more authority to states. The ESSA requires that child welfare agencies and school districts develop a joint plan to ensure that transportation is available when it is in a student's best interest to remain in their School of Origin after a change in placement.

3.5 Families First Prevention Services Act (FFPSA):

3.5.1 Federal law enacted in 2018 (Public Law 115-123), which amended existing provisions within Title IV-B and IV-E of the Social Security Act and established new preventive service options and requirements for foster care placement settings.

3.5.2 Under FFPSA, federal financial resources may be available to child welfare jurisdictions for kinship navigator services and select evidenced-based prevention services to strengthen families and communities, including behavioral health and substance abuse prevention and treatment services, and in-home parenting skill-based programs for children or youth who are candidates for foster care, pregnant or parenting youth in foster care, and the parents or kin caregivers of those children and youth.

3.5.3 Implementation of FFPSA establishes new processes to ensure that any Title IV-E eligible child placed in a Short-Term Residential Therapeutic Program (STRTP) facility that meets the federal Qualified Residential Treatment Program (QRTP) standards requires the level of treatment intervention offered by that STRTP. Within 30 days of entering the facility, the child must receive an assessment from a qualified individual using an appropriate functional assessment tool to determine whether STRTP care is necessary and whether that particular residential facility can meet the child's specific treatment needs.

3.6 Integrated Core Practice Model (ICPM): A comprehensive, trauma-informed framework for child-serving agencies, mandated by WIC Section 16521.6(a)(2)(C) to ensure integrated, collaborative service delivery. The ICPM provides practical guidance and direction to support county child welfare, juvenile probation, behavioral health staff, and community partners in using best practices for the delivery of timely, effective, and collaborative services.

3.7 Intensive Services Foster Care (ISFC): A private nonprofit or public agency program model of home-based family care for eligible children whose needs for safety, permanency, and well-being require specially trained resource parents, and intensive professional and paraprofessional services.

3.8 Non-Minor Dependent (NMD): Pursuant to WIC §11400(v), a dependent or ward of the juvenile court, or a non-minor under the transition jurisdiction of the juvenile court, who has attained the age of 18 years while in foster care and is eligible for extended foster care.

3.9 Resource Family: A caregiver who provides out-of-home care for children in foster care. Resource Families include individuals, couples, and families. They may be related, have a familiar or mentoring relationship, or have no previous relationship with the child.

3.10 School of Origin (SOO): The school a student attended when permanently housed or the school in which they were last enrolled, including preschools, which ensures educational stability for homeless or foster youth, allowing them to remain in their original school despite changing living situations or districts.

3.11 Short-Term Residential Therapeutic Program (STRTP): A residential facility licensed by the California Department of Social Services (CDSS) and operated by a public agency or private organization, to provide specialized 24-hour care and supervision, treatment, services, and supports to children and NMDs.

3.12 Therapeutic Foster Care (TFC): Short-term, intensive, highly coordinated, trauma-informed, and individualized rehabilitative services covered under Medi-Cal that are provided to youth up to 21 years of age, with complex emotional and behavioral needs, who are placed with trained and supported TFC resource parents.

3.13 Trauma-Informed Model: A response model that fully integrates knowledge about trauma into interventions and engagement strategies.

3.14 Wraparound:

3.14.1 Family-focused, strength-based, needs-driven, team-oriented collaborative, and coordinated system of support for children and families.

3.14.2 Comprises family members, friends, service providers, peer specialists, advocates, and other members of a family's community.

3.14.3 The goals include addressing crises in order to keep reunified children with their respective parents and to maintain children in the least restrictive, most family-like setting possible, ideally within their own communities.

3.14.4 The process provides an array of services and supports, including, but not limited to, respite, case management activities, support groups, advocacy, treatment, family training, home/school services, behavioral health services, and coordination with community services.

4. TARGET POPULATION

4.1 Children and youth in Orange County, including, but not limited to, children and youth in foster care, NMDs, children, youth and families who have experienced severe trauma or are at risk of future trauma, and may be involved in or are at risk of being involved in the child welfare and/or probation systems in Orange County.

5. GOVERNANCE STRUCTURES AND SCOPE OF AUTHORITY

5.1 Interagency Leadership Team (ILT)

The ILT shall:

5.1.1 Serve as the leadership team of this collaborative effort.

5.1.2 Consist of the SSA Child Welfare Director, or designee; HCA Deputy Agency Director, or designee; Chief Probation Officer, or designee; OCDE Superintendent of Schools, or designee; RCOC Executive Director, or designee; and First 5 Orange County Chief Executive Officer, or designee.

5.1.2.1 While leadership of the ILT is established per Subparagraph 5.1.2 of this MOU, ILT meetings may also be attended by others as needed and determined by the ILT members, including, but not limited to, designated staff or senior managers of the Parties, other involved agencies, Local Education Agency (LEA), Managed Care Plan organizations, tribal partners, faith-based partners, or identified contractors, foster youth, resource family, and/or birth parent representative.

5.1.3 Select a Chair to lead ILT meetings and processes, and to coordinate meeting venues and notifications for a period of two years. Meeting processes may include, but are not limited to: securing meeting venues, determining the forum of the meetings, facilitating communication of relevant information and updates among the ILT in between scheduled meetings, recording meeting minutes/decisions, and coordinating with the ILT to identify parties responsible to advance recommendations.

5.1.4 Hold ILT meetings at minimum on a quarterly basis.

5.1.5 Attend all meetings and planning sessions necessary to mutually carry out their shared mission and goals set forth in this MOU.

5.1.6 Utilize a shared decision-making process. Consensus will be the preferable model for the ILT; however, if consensus cannot be reached and a quorum has been established, decisions may be made by a majority vote of the ILT members.

5.1.6.1 Decisions of the ILT are advisory and not binding on any Party.

5.1.7 Engage in an ongoing review of its procedures to ensure that this MOU remains current.

5.1.8 Abide by and support the actions and principles of Attachment A of this MOU (Tribal Consultation Policy).

5.2 ILT Advisory Committee (IAC)

5.2.1 The ILT leadership members may determine and appoint an IAC of individuals serving in a leadership capacity among the Parties to assume the duties and responsibilities prescribed by the ILT.

5.2.2 The IAC will communicate identified gaps in continuity of care, quality improvement recommendations, and/or training and technical assistance to the ILT for review and consideration to support the programs and services identified within the Trauma-Informed System of Care.

5.3 Interagency Placement Committee (IPC)

5.3.1 The IPC will include a representative from:

5.3.1.1 The County placing agency (i.e., SSA or Probation);

5.3.1.2 The County Behavioral Health Plan; and

5.3.1.3 A representative from both SSA and Probation for WIC §241.1 Dual Status cases.

5.3.2 While composition of the IPC is established per the above provisions, IPC meetings may be attended by others as needed and determined by the IPC, including, but not limited to: assigned social worker, OCDE and/or school district representative, assigned probation officer and/or supervisory staff, Wraparound representative, and STRTP placement staff.

5.3.3 HCA participation in the IPC is limited to providing clinical input within its scope of practice and does not confer placement authority or responsibility. The role of the Behavioral Health Plan representative on the IPC is advisory and distinct from the placement functions of the placing agencies.

5.3.4 The IPC will communicate identified gaps in continuity of care, quality improvement recommendations, and/or training and technical assistance to

the ILT and/or IAC for review and consideration, to support the programs and services identified within the Trauma-Informed System of Care.

5.3.5 Pursuant to WIC §§4096 and 11462.01, the requirements for placing a child/NMD into an STRTP includes a formal assessment by the IPC.

5.3.5.1 If a CFT finds STRTP placement necessary, a referral is submitted to initiate IPC review to determine whether criteria for STRTP placement are met and whether the needs of the child/NMD would be best served in an STRTP.

5.3.5.2 The IPC will review the service plan and consider behavioral supports and/or therapeutic treatment that may be recommended to maintain the child/NMD in the least restrictive setting.

5.3.5.3 Following placement into an STRTP, the IPC may support the CFT in re-assessing the appropriateness of the STRTP placement to consider when home-based care may be feasible, and to identify aftercare services to support a transition to a lower level of care.

5.3.6 The Parties agree to follow and if necessary, jointly modify the protocols addressing IPC-related processes, based on legislative and regulatory changes stemming from FFPSA, as it relates to placement of a Title VI-E eligible child in a STRTP facility that meets the federal requirements of a QRTP, detailed in:

5.3.6.1 STRTP and IPC Desk Guides;

5.3.6.2 IPC Approval Process for STRTP Placement;

5.3.6.3 Documentation Requirements and Extension Criteria for STRTP Placement;

5.3.6.4 IPC Referral for STRTP Placement (F063-25-826); and

5.3.6.5 Deputy Director Approval STRTP Placement Extension (F063-25-743).

5.3.7 IPC Case Specific Appeals

A staff member associated with the child/NMD's care who disagrees with an IPC recommended action may raise an objection to the recommended action, or may advocate for a different action using the appeal process as outlined herein:

5.3.7.1 Within two business days of the IPC meeting, the staff member wishing to appeal the IPC recommendation(s) will notify and submit a brief memo to their supervisor/manager, describing the desired action and reason(s) for the appeal request.

5.3.7.2 Following the review, the supervisor/manager will determine whether to formally request an appeal. Should an appeal be requested, the memo will be forwarded to the appropriate IPC representative(s).

5.3.7.3 Within two business days of receiving the memo, the IPC representative will attempt to resolve the concern(s), in consultation with the requestor and the IPC representative.

5.3.7.4 If consensus cannot be reached within the IPC, the IPC will update the memo with additional remarks identifying the factors the IPC considered when making its recommendation(s).

5.3.7.5 Within two business days, the IPC representative will forward the appeal for review and resolution to the following individuals, as applicable: Chief Deputy Probation Officer (Juvenile Operations), or designee; Child Welfare Deputy Director, or designee; and Children and Youth Behavioral Health Division Manager, or designee.

5.3.7.6 The individuals described in Subparagraph 5.3.7.5 of this MOU may consult with the ILT and/or IAC in response to the appeal. The ILT and/or IAC may review the appeal and may invite stakeholders to present information, as necessary.

5.3.7.7 A shared decision-making process will be utilized, and consensus will be sought among the appeal panel.

6. ROLES AND RESPONSIBILITIES

6.1 ILT Management, Administration, and Service Delivery

6.1.1 Provide oversight and administrative planning to support the Orange County Trauma-Informed System of Care.

6.1.2 Analyze opportunities, projects, and recommendations submitted to the ILT for review.

6.1.3 Assign staff, subject to available resources and funding, as needed to support shared programming, including technical assistance and training, program coordination, problem-solving, and staffing needs.

6.1.4 Promote alignment of staff and programs with the shared vision, mission, purposes, and principles of this MOU.

6.2 ILT Exchange of Information

6.2.1 Members of the ILT may, to the extent permitted by federal law and subject to the limitations set forth in Subparagraph 2.4.5 et seq., disclose to and

exchange with one another any information or writing designated as confidential under State law, provided that the member possessing such information or writing reasonably believes it is relevant to the identification, reduction, or elimination of barriers to services or placements for children, youth, and NMDs in foster care, or to improve provision of such services or placements.

6.2.2 Members of the ILT who receive information or writings disclosed or exchanged pursuant to Subparagraph 2.4.5 et seq. shall destroy or return such information or writings once the purposes for which they were disclosed or exchanged have been satisfied. Such information or writings shall be used only for the purposes described in Subparagraph 2.4.5 et seq. Any information or writings disclosed or exchanged shall be confidential and shall not be open to public inspection unless aggregated and deidentified in a manner that prevents the identification of any individual who is the subject of the information or writings. Any discussion of such disclosed or exchanged information or writings during a team meeting shall be confidential and shall not be open to public inspection.

6.3 Policy Development, Coordination, and Monitoring as a Trauma-Informed System of Care

6.3.1 Provide guidance and direction, as needed, on implementation of policies, procedures, and programs included under this MOU.

6.3.2 Make recommendations regarding submission, preparation, and coordination of grant applications and grant deliverables which affect the processes and/or services of interrelated Parties.

6.3.3 The Parties may develop additional MOUs, contracts, or policies and procedures.

6.3.3.1 Where such documents may directly affect the operations or obligations of any Party, the procedures established for joint review and approval shall also apply.

6.3.3.2 These documents may address lines of operational authority or shared authority among directors, departments, and/or managers.

6.3.4 Participate in related coordinating councils, other advisory committees, and multi-disciplinary teams which affect the Trauma-Informed System of Care processes and/or services.

6.3.5 Appoint and support staff to monitor programs for general compliance with statutory and regulatory requirements.

6.3.6 Provide guidance and technical assistance to ensure program practices are

consistent with the values and principles of this MOU.

6.3.7 Work with community agencies to ensure collaborative and integrated strategies are utilized to promote strength-based and family-focused practices on a systemwide basis.

6.3.8 Provide reviews and suggestions, as necessary, for program direction for applicable community partners and/or providers.

6.3.9 Ensure compliance with the actions and principles set forth in Attachment A of this MOU (Tribal Consultation Policy) and provide guidance and technical assistance as needed.

6.4 Screening and Assessment for Entry into Care and Service Alignment

6.4.1 The Parties shall support the use of or utilize integrated screening processes and assessments, consistent with clinical and regulatory requirements, to identify the individual needs of the Target Population who have experienced severe trauma or are at risk of future trauma, and to enhance unified service planning, coordinate care, avoid duplication of services, and reduce administrative costs to partners.

6.4.2 The Parties agree to use the following screening, assessment, and care planning tools as applicable to each Party's programs and services, and to share assessment outcomes and processes, where possible, to facilitate timely unified service planning and care coordination. Such screening, assessment, and care planning tools may be replaced with comparable or superior measures at the discretion of the respective Parties, in consultation with collaborative partners or pursuant to a mandate from the State.

6.4.2.1 SSA: CANS, Structured Decision Making, Level of Care, Specialized Care Increment, Child Welfare Case Plan, Plan of Safe Care, CFT Plan, Needs and Services Plan, Transitional Independent Living Plan (TILP), and/or Supervised Independent Living Plan (SILP).

6.4.2.2 Probation: CFT Plan, Needs and Services Plan, Juvenile Placement Case Plan, TILP, and/or SILP.

6.4.2.3 HCA: IP-CANS, Pediatric Symptom Checklist-35, Decision Support Criteria (DSC), Youth Outcomes Questionnaire, CRAFFT - Care, Relax, Alone, Forget, Friends, Trouble, Substance Abuse Choices Scale-B, Commercial Sexual Exploitation – Identification Tool, American Society of Addiction Medicine, and Multi-Dimensional Assessment for Substance Use Disorder/Diagnosis, psychosocial assessment, and care plan.

6.4.2.4 OCDE: Individualized Education Program (IEP), Section 504 Plan, Student Study Team/Student Success Team/Student Intervention Team documents, attendance records, discipline records, and/or report cards/transcripts.

6.4.2.5 RCOC: Individual Program Plan.

6.4.3 The Parties agree to examine the continuum of programs each Party has at their disposal in order to:

6.4.3.1 Compile a listing of available educational, health, child welfare and placement continuum service delivery options and associated legal timelines, where applicable.

6.4.3.2 Support ongoing efforts to identify and address potential gaps in the existing service/placement array.

6.4.4 The Parties shall establish agreements and protocols, as needed and in accordance with Subparagraph 2.4.5 et seq., to enable the lawful sharing of client-related information such that assessment and planning documents may be accessed by each Party's service personnel within the scope of their assigned duties.

6.5 CFT and Unified Service Planning

The Parties agree to:

6.5.1 Provide a single, unified teaming process for the Target Population, to the extent permitted by each Party's legal, regulatory, and funding requirements and individual discretion.

6.5.2 Support family-centered teaming, planning, and engagement in a manner that acknowledges family voice, choice and individualized needs; involve formal and natural supports as members of the CFT based on family preference; address timeframes and circumstances necessitating a CFT meeting; and promote cross-system unified service planning and care coordination to help families reach their goals.

6.5.3 Follow CFT policies outlined by the applicable State agency, including, but not limited to, CDSS, California Department of Health Care Services, California Department of Corrections and Rehabilitation, California Department of Education, and California Department of Rehabilitation.

6.5.4 Follow specific agency policies identified in the SSA CFS Policy and Procedure for CFT (D-0314) and the HCA Behavioral Health Services Policy and Procedure for Pathways to Well Being and Intensive Services 01.02.06.

6.5.5 Where applicable, any information that includes substance use disorder

treatment records shall be made only in accordance with 42 CFR Part 2. All disclosures requiring individual authorization shall be supported by a valid, written authorization in compliance with HIPAA and 42 CFR Part 2.

6.5.6 Jointly modify policies related to CFT-related processes in response to current and future legislative or regulatory changes, including but not limited, to those stemming from FFPSA, as they pertain to placement of a Title VI-E eligible child in an STRTP facility that meets the federal requirements of a QRTP.

6.5.7 Authorize the participation of a qualified LEA representative in CFT Meetings. The representative shall possess sufficient knowledge about the child and be able to provide feedback on the following:

6.5.7.1 Significant relationships that the child may have formed or established, including but not limited to, relationships with teachers, counselors, coaches, or other meaningful individuals involved in the child's academic or extracurricular life.

6.5.7.2 The potential impact of any proposed school change on the child's academic performance, social development, and/or emotional well-being.

6.5.8 Share relevant IEP-related information necessary to inform service planning and delivery with members of the CFT, where permissible and in compliance with applicable privacy laws, security policies, and confidentiality standards for data sharing as outlined in Subparagraph 2.4.5.

6.6 School Stability, Supports and School of Origin (SOO) Transportation Plan

To comply with ESSA and improve school stability for students in foster care, the Parties agree to develop and enact joint policies and procedures to ensure:

6.6.1 LEAs, school districts, and schools receive notice of any decision by the child welfare agency to change a student's placement, and whenever feasible, before the placement change occurs.

6.6.2 The Parties work with the youth and the youth's education rights holder, if applicable, to promptly make a best-interests determination.

6.6.3 Students receive transportation to their SOO during the pending best-interests determination and throughout any pending dispute resolution regarding SOO rights.

6.6.3.1 If it is determined to be in the student's best interest to remain in their SOO, transportation shall be provided by the child welfare agency (e.g., caregiver reimbursement, public bus passes), by the school district in accordance with Education Code Section 48850

et seq. (e.g., use or modification of an existing bus route), or through a jointly agreed-upon arrangement between the child welfare agency and the school district (e.g., cost-sharing through social worker transport or contracted services).

6.6.4 The prompt transfer of educational records for students in foster care when they enter or exit a school, whether within the same LEA or between LEAs.

6.6.5 Immediate enrollment for students in foster care who enter a school within the LEA.

6.6.6 Immediate education records requests from the SOO for students in foster care who enroll in a school within the LEA.

6.6.7 Students in foster care are promptly enrolled in the LEA's free lunch program.

6.6.8 Students in foster care shall not owe or be billed for any debt to a school or district. If a student has an outstanding debt, the school or district shall not take negative action against a student, including withholding grades, transcripts, or a diploma. This provision applies to students in foster care regardless of whether the student has willfully damaged or failed to return school property.

6.7 Implementation of California Integrated Core Practice Model (ICPM)

6.7.1 This MOU affirms the Parties' shared commitment to the principles of the ICPM and its application in serving children and youth currently in, or at risk of, foster care who have experienced severe trauma, as well as their families. The ICPM outlines the shared values, core components and standards of practice expected from all parties serving California's children, youth, NMDs, and families.

6.7.2 The Parties agree to establish processes to ensure that staff assigned to shared programming supporting a Trauma-Informed System of Care are informed of, and promote, the purpose, role, and integration of the ICPM.

6.7.3 The Parties agree to mutually apply the principles, values, and practice behaviors in their interactions with youth and family, with one another, and with contractors and partners.

6.7.4 The ICPM is further supported by the Parties through use of the California Integrated Training Guide, as outlined in the State of California, Health and Human Services Agency All-County Information Notice I-21-18.

6.7.5 The Parties acknowledge that ICPM integration is an ongoing process and, as needed, will utilize planning guidance and other relevant resources available through the California Social Work Education Center to

implement and/or advance ICPM within cross-system collaborative efforts.

6.8 Recruitment and Management of Resource Families and Delivery of TFC

6.8.1 The Parties are committed to collaborating and supporting the recruitment, training, and retention of Resource Family caregivers to foster safe, permanent, and healthy options for out-of-home care.

6.8.2 SSA and Probation have legal obligations to ensure the availability of foster care resources and placement capacity.

6.8.3 HCA has parallel responsibility to ensure adequate capacity for, and oversight of, Specialty Mental Health Services and Drug Medi-Cal Services necessary to support youth and their caregivers.

6.8.4 The Parties agree to share necessary information and processes, as permitted by law, to strengthen identification, recruitment, and retention efforts to build the capacity of Resource Families, TFC, ISFC, and STRTPs serving foster youth.

7. INFORMATION AND DATA SHARING

7.1 The Parties agree to develop information and data sharing agreements in accordance with the standards and principles set forth in Subparagraph 2.4.5, above, and such other additional laws, regulations, standards, local rules, or principles that legally govern the disclosure, use, and sharing of such information and data as related to this MOU.

7.2 The Parties may utilize secure, mutually agreed-upon data sharing platforms to exchange information necessary to support the mission and activities of this MOU including, but not limited to, document repositories, shared drives, and collaborative workspaces. Any platform used for data exchange shall meet all applicable federal, State, and County requirements related to privacy, confidentiality, and information security.

7.2.1 Use of any data sharing platform under this MOU shall be reviewed and approved by each Party's respective Information Technology department to ensure that the platform includes appropriate security controls and safeguards to comply with agency-specific security standards.

7.2.2 Each Party shall ensure that only authorized personnel access such platforms, and such use shall comply with the confidentiality, security, and information-sharing provisions of this MOU.

8. QUALITY MANAGEMENT AND PROVIDER OVERSIGHT

8.1 The Parties shall maintain their respective and collective responsibilities related to tracking, monitoring, evaluating, and reporting on their services.

8.1.1 As needed or required, the Parties shall report information to State agencies.

8.1.2 As needed or required, the Parties shall fulfill any additional responsibilities related to evaluation of contractors and vendors.

8.2 While these requirements vary in form and process, the Parties recognize that certain critical areas present opportunities to strengthen shared goals and enhance fiscal efficiency.

8.3 The Parties agree to share relevant findings, data, and/or recommendations derived from a range of sources, as allowed by law, including, but not limited to System Improvement, Child Family Services Review, Case Review, External Quality Review Organization, Local Accountability Plans, and Triennial Behavioral Health Plan Review. The Parties further agree to identify opportunities for coordinating and sharing resources and processes to support a Trauma-Informed System of Care.

8.3.1 HCA's participation in shared evaluation activities shall be limited to data and reporting permissible under applicable privacy laws.

8.4 The Parties agree to invite stakeholders, coordinating councils, and other advisory committees to present regular reports on progress, outcomes and/or identified gaps in continuity of care related to implementation of services, supports, and programs associated with CCR and/or a Trauma-Informed System of Care.

9. STAFF RECRUITMENT, TRAINING, AND COACHING

9.1 The Parties acknowledge the importance in maintaining highly trained and competent staff teams. To ensure that providers of critical services, including, but not limited to, social workers, probation officers, physical and behavioral health professionals, educational professionals, development disability professionals, and support and administrative personnel are fully prepared to deliver the seamless and integrated services described in this MOU, the Parties agree to coordinate the recruitment, training, and coaching of staff in a manner that promotes effective cross-system collaboration.

9.2 The Parties agree that, when feasible, training and/or in-service activities that may benefit Party staff or other key partners, shall be jointly planned and delivered through coordinated, cross-training processes.

9.3 The Parties acknowledge a mutual commitment to cross-train staff on the shared values, core components, and standards of practice of the ICPM.

9.4 The Parties agree that modalities for cross-training may include, but are not limited to, classroom learning, e-learning and webinar formats, coaching, and mentorship opportunities.

9.5 The Parties agree that financial training resources shall be utilized in the most flexible and adaptable manner possible to facilitate the cross-training and

preparation of staff.

10. FINANCIAL RESOURCE MANAGEMENT

10.1 Notwithstanding the generally categorical nature of each Party's revenues, the Parties will inform the ILT membership about all available, applicable funding resources related to this MOU. This includes State and federal revenues, ongoing funding, one-time funding opportunities, potential revenue enhancements, Request for Proposals, and grant opportunities for programs and services for the Target Population.

10.2 Funding may consist of federal, State, local, or private resources within the discretion of the Parties, and will be sought or applied for, planned, monitored, and distributed with consideration of input from and/or recommendations provided by the ILT.

10.3 Funding decisions subject to approval by the governing body of each Party may be brought to those governing bodies with an accompanying recommendation from the ILT.

10.4 The Parties agree to identify and address barriers to cost-sharing and to promote the use of creative fiscal strategies that responsibly leverage available financial resources to provide the Target Population with timely access to an array of quality services within the Trauma-Informed System of Care.

10.5 Although this MOU is non-financial, the Parties may, at their discretion and subject to available appropriations and internal budgetary authority, allocate or utilize their own funds to support consultant services or other necessary costs associated with implementing the collaborative activities under this MOU. Any such contributions are voluntary and contingent upon the availability of agency resources, and no Party is required to commit funds beyond those it elects to make available.

11. NON-DISCRIMINATION

11.1 In the performance of this MOU, the Parties agree to 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.

12. CONFIDENTIALITY

12.1 The Parties agree to follow confidentiality laws, regulations and procedures as

stated in Subparagraph 2.4.5 of this MOU and maintain confidentiality of records relating to this MOU, to the extent permitted by law.

12.2 All records and information concerning any and all persons served through programs under the guidance of this MOU shall be considered and kept confidential by each Party's employees, agents, subcontractors, and all other individuals performing services under this MOU. Each Party shall require its employees, agents, subcontractors, and all other individuals performing services under this MOU agree to maintain the confidentiality of any client-specific data received pursuant to this MOU.

12.3 Each Party 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. Failure to maintain confidentiality of the information received pursuant to and for purposes of this MOU may subject the breaching Parties and all of its employees, agents, and all other individuals performing services under this MOU to potential criminal and civil liabilities pursuant to WIC Sections 827, 832, 827.9, 828.1, 10950, and 18968.46.

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

12.4.1 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.

12.4.2 Each Party 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.

13. MUTUAL HOLD HARMLESS

13.1 The Parties signing this MOU agree that each Party will be responsible for its own acts and omissions, be responsible for the acts and omissions of its employees, officers, and officials ("Employees"), and shall not be responsible for the acts or omissions of the other Parties or the other Party's Employees.

13.2 These obligations relate to any and all claims, lawsuits, actions, or special proceedings, whether judicial or administrative in nature, and include any loss, liability, or expense, including reasonable attorney's fees, relating to this MOU

("Claims").

13.3 Employees of each Party shall not be considered employees or joint employees of the other Parties for purposes of workers' compensation, common law employment or statutory employment obligations or benefits.

14. SECURITY

14.1 SSA, HCA, Probation, OCDE and First 5 Orange County shall abide by the requirements in Attachments C and D, incorporated by reference to the MOU and attached hereto. For the purposes of this MOU, any reference to "Contractor" within Attachments C and D shall be interpreted to mean SSA, HCA, Probation, OCDE and First 5 Orange County.

15. NOTIFICATION OF INCIDENTS, CLAIMS, OR SUITS

The Parties shall report to each other, in writing, within 48 hours of occurrence, excluding weekends and holidays, the following:

15.1 Any accident or incident relating to duties performed under this MOU that involves injury or property damage which may result in the filing of a claim or lawsuit against any of the Parties.

15.2 Any third-party claim or lawsuit filed against any of the Parties arising from or relating to duties performed by any of the Parties under this MOU.

15.3 Any injury to an employee of any of the Parties that occurs on the property of any of the Parties.

15.4 Any loss, disappearance, destruction, misuse, or theft of any kind whatsoever of the property, monies, or securities entrusted to any of the Parties under the term of this MOU.

16. NOTICES

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

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

County of Orange Health Care Agency
Contracts Services
405 W. 5th Street
Santa Ana, CA 92701

Orange County Probation Department
Contracts Department
1055 N. Main St., 5th floor
Santa Ana, CA 92701

Orange County Department of Education
Contracts Department
200 Kalmus Drive
Costa Mesa, CA 92628-9050

Regional Center of Orange County
1525 N. Tustin Avenue
Santa Ana, CA 92705

First 5 Orange County
1505 E. 17th Street, Suite 230
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.

17. RESOLUTION OF CONFLICTS

17.1 While ILT member agencies and leaders will utilize a shared decision-making process for programs and services related to this MOU, the Parties acknowledge that challenges and disagreements may arise, including those stemming from conflicting policies, guidance, or differing opinions. The Parties shall make good faith efforts to resolve any dispute or disagreement arising under this MOU.

17.2 For disputes involving policy, direction, sharing of resources, strategy or related cross agency issues related to this MOU, the Parties will seek to resolve such matters by focusing on the shared vision, values, and practices of this agreement. The Parties acknowledge that youth and family members are generally unaware of and have no particular interest in which agency bears greater or lesser responsibility for their care, and that decisions should therefor prioritize their experience and well-being.

17.3 The Parties acknowledge that in some cases, once local resolution processes have

been exhausted, referral to the Children and Youth System of Care State Technical Assistance Team may be considered. In such instances, the Parties agree to follow the guidance set forth in All County Letter 20-63 and Behavioral Health Information Notice 20-013.

17.4 Performance of this MOU shall continue during any dispute resolution proceeding or any other mechanism used to address disagreements.

18. CONFLICT OF INTEREST

18.1 The Parties shall exercise reasonable care and diligence to prevent any actions or conditions that could result in a conflict with the best interests of County. This obligation shall apply to each Party's officers, directors, employees, agents, and subcontractors associated with accomplishing work and services hereunder. The Parties' efforts shall include, but not be limited to, establishing precautions to prevent its employees, agents, and subcontractors from providing or offering gifts, entertainment, payments, loans or other considerations which could be deemed to influence or appear to influence County staff or elected officers from acting in the best interests of County.

18.2 The Parties shall notify County, in writing, of any potential or actual conflicts of interest between the Parties 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, each Party. While each Party will be required to provide this information without prompting from County any time there is a change regarding conflict of interest, the Parties must also provide an update to County upon request by County.

19. TERMINATION

19.1 A Party mandated by law shall remain a Party to this MOU for as long as such mandate remains in effect. A mandated Party may terminate its participation only if permitted by applicable law or State directive and shall provide 30 days' written notice to the other Parties identifying the statutory or regulatory basis for termination.

19.2 A Party not mandated by law may terminate its participation in this MOU at any time by providing 30 days' written notice to the other Parties.

19.3 If a mandated Party terminates its participation pursuant to applicable law or State directive, and such termination is concurred with and formally authorized by the other Parties, the remaining Parties shall collaborate to identify and engage the appropriate successor entity required by law to fulfill the mandated role. The MOU shall be amended as necessary to incorporate the successor entity and ensure

continuity of required functions.

19.4 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.

20. 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. The Parties represent and warrant that the person executing this MOU on behalf of and for their respective Party is an authorized agent who has actual authority to bind the Party to each and every term, condition and obligation of this MOU and that all requirements of the Parties have been fulfilled to provide such actual authority.

21. GENERAL PROVISIONS

21.1 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 the Parties' agents or employees.

21.2 This MOU, with its Attachments(s) 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.

21.3 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.

21.4 In the performance of this MOU, the Parties shall comply with all applicable laws and regulations of the United States, State of California, and all administrative regulations, rules, and policies adopted thereunder, that relate to this MOU, as each and all may now exist or be hereafter amended.

21.5 In the performance of this MOU, no Party may delegate its duties or obligations nor assign its rights, either in whole or in part, without the prior written consent of the other Parties. Any attempted delegation or assignment without prior written consent shall be void.

21.6 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.

By: _____

An Tran
Director
County of Orange, Social Services Agency

Dated: _____

By: DocuSigned by: Veronica Kelley
E8B80965A4EC417...

Veronica Kelley
Director
County of Orange, Health Care Agency

Dated: 8/15/2026 | 8:11:11 PM PDT

By: DocuSigned by: Daniel Hernandez
94A0CE1925D14F3...

Daniel Hernandez
Chief Probation Officer
County of Orange, Probation

Dated: 8/6/2026 | 11:43:31 AM PDT

By: Signed by: Pat McCaughey
811F9701E03F4D6...

Pat McCaughey
Director
Orange County Department of Education

Dated: 8/4/2026 | 1:31:06 PM PDT

By: DocuSigned by: Larry Landauer
E3981964CF7A43C...

Larry Landauer
Executive Director
Regional Center of Orange County

Dated: 7/28/2026 | 12:44:03 PM PDT

By: Signed by: Kimberly Goll
2651BE09D88E4C6...

Kimberly Goll
President/Chief Executive Officer
First 5 Orange County

Dated: 7/28/2026 | 11:32:44 AM PDT

APPROVED AS TO FORM
COUNTY COUNSEL
COUNTY OF ORANGE, CALIFORNIA

Carolyn S. Frost
Print Name

Deputy County Counsel
Title

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

7/28/2026 | 11:21:51 AM PDT
Date

ATTACHMENT A

THE COUNTY OF ORANGE, INTERAGENCY LEADERSHIP TEAM

TRIBAL CONSULTATION POLICY

ASSEMBLY BILL 2083 TRIBAL CONSULTATION POLICY

This Tribal Consultation Policy is a model designed to assist Interagency Leadership Teams (ILTs), in consultation with Tribes, to tailor their own Consultation efforts, resources, and timelines. This document is consistent with the California Department of Health and Human Services Tribal Consultation Policy and the California Department of Social Services Tribal Consultation Policy.

Sections:

This Tribal Consultation Policy (TCP) is entered into by and between the County of Orange (County) Social Services Agency, County Probation Department, County Health Care Agency, Orange County Department of Education, and Regional Center of Orange County, collectively named the Interagency Leadership Team, hereinafter referred to as "ILT," and tribal entities, individually or collectively including, but not limited to, local Tribes, state recognized Tribes, and federally recognized Tribes or sovereign nations with tribal members or membership-eligible children and families within Orange County, hereinafter referred to as "Tribes". This TCP establishes the procedures for the ILT (and/or designated representatives of each ILT agency/department) to engage in regular, meaningful, and robust consultation with tribal officials in the development of local programs, policies and practices that have tribal implications.

The ILT and Tribes may be referred to individually as "Party" and collectively as "the Parties." The relationship between the Parties, with regard to this TCP, is based upon the following:

1. PURPOSE:

California counties fulfill a vital role in the state's efforts to serve its most needy and vulnerable residents and play a key role in meeting federal and state requirements and policies, including consultation with Tribes.

The purpose of this TCP is to:

a. Guide effective government-to-government consultations between the Parties;

b. Outline a process for Tribes to provide meaningful input into the development of local programs, policies, and practices that affect tribal communities and tribal children/families; and

c. Create opportunities for the ILT to learn from tribal program experience in a manner that informs program operations and policy development.

This TCP is consistent with California Gubernatorial Executive Order B-10-11, September 19, 2011, and the subsequent development of the California Health and Human Services Agency California Health and Human Services Agency Tribal Consultation Policy and the California Department of Social Services (CDSS) Tribal Consultation Policy. It is also consistent with the mandate set forth in W.I.C. §16521.6 requiring the System of Care Memorandum of Understanding (MOU) to contain processes as developed through tribal consultation with Tribes within each County, and for engaging and coordinating with these Tribes in the ongoing implementation of the MOU.

2. SCOPE:

This TCP applies to the Trauma Informed System-of-Care Foster Youth MOU executed on August 27, 2021, and shall serve as a guide to facilitate tribal engagement around development of local System of Care programs and policies before action is taken, to the greatest extent practicable and permitted by law.

This TCP facilitates inclusive collaboration and informed decision-making. Parties will promote respect, shared responsibility, transparency, open communication and free exchange of information. Meaningful consultation begins at the earliest possible phase of project or program planning and continues through each phase of development and implementation to promote effective policies and programs with positive outcomes for tribal communities and tribal children/families. The Parties will also recognize and respect diverse tribal customs and traditions, which may be especially applicable to inform programs and policies that include provision of services.

This TCP is not intended and should not be construed to define a legal relationship between the ILT and its departments and Tribes. This policy does not create, expand, limit, waive, or interpret any legal rights or obligations, including State, county, or tribal governmental rights, sovereign immunity, or jurisdiction.

This TCP is not intended to preclude collaborative relationships between the ILT and any Tribe(s) outside of the processes described in this policy. The feedback and recommendations received through collaboration activities are intended to inform the Parties on issues relevant to tribal communities and tribal children/families to support formal government-to-government consultation with Tribes.

3. DEFINITIONS:

a. Collaboration: Working together in a meaningful effort to create a positive outcome. Collaboration occurs with authorized representatives from each party (e.g., staff acting

within the scope of their authority) who effectuate the policy objectives identified and determined through Consultation as described under the Process and Procedure section.

b. Consultation: A formal process of government-to-government communication among leadership within the Tribes and System of Care Partners that emphasizes trust, respect, and shared responsibility. It is an equitable, open, and free exchange of information and opinion among parties, with the goal of attaining mutual understanding and informed decision-making.

c. Federally Recognized Tribe: A Native American Tribe with whom the federal government maintains an official government-to-government relationship. The Bureau of Indian Affairs maintains and regularly publishes the list of federally recognized Indian Tribes in the Federal Register and maintains a directory on its website.

d. Indian Organizations: A group, association, partnership, corporation, or other legal entity owned or controlled by Indians, or a majority of whose members are Indians who serve and advocate and/or act in an advisory capacity for concerns and issues impacting Tribes and tribal children and families in California.

e. Indians: American Indians and Alaska Natives (AI/AN), also referred to as Native Americans, and any descendant of a Tribe indigenous to the United States.

f. Interagency Leadership Team (ILT): An administrative body with collaborative authority over the interrelated child welfare, juvenile justice, education, developmental, and children's behavioral health services in Orange County.

g. Interagency Leadership Team (ILT) Advisory Committee (IAC): A group comprising individuals serving in a leadership capacity as determined by the ILT, to assume the duties and responsibilities prescribed by the ILT.

h. Local Tribes: State or federally recognized tribes that reside within Orange County, including tribal members or membership-eligible children and families that may be living in Orange County under another state's proclamation.

i. Significant Actions: "Significant actions" refer to policies or program activities that:

   i. have tribal implications; and

   ii. have substantial direct effects on (a) one or more Tribe(s) and Indian Organizations, or (b) the relationship between the County government and Tribe(s) and Indian Organizations, or (c) the distribution of power and responsibilities between the County government and Tribe(s) and Indian Organizations; or

   iii. have an effect on or influence Tribe(s) and Indian Organizations in the County.

j. State-Recognized Tribes: Non-federally recognized Native American Tribes that do not meet the criteria for federally recognized Indian tribes but have been recognized by a process established under a range of state government laws for varying purposes. State recognition does not dictate whether or not they are recognized as Native American Tribes by continually existing tribal nations.

k. System of Care: Collaborative work with state, county, and local partners which aims to ensure that program services provided to children and families by placing agencies (child

welfare or probation), education, county behavioral health, and local regional center are coordinated, timely, and trauma informed.

l. To the Extent Practicable and Permitted by Law: Refers to situations where the opportunity for Consultation is limited because of constraints of time, budget, legal authority, or other situations beyond the control of the parties.

m. Tribal Partner: Any Tribe(s) or Indian Organization(s) participating in the Tribal Consultation Policy and related efforts or actions within the System of Care.

n. Tribal Representative or Tribal Designee: The elected Tribal Chairperson or their designee by resolution or letter.

4. TRIBAL LIAISON:

The ILT Chairperson(s) shall designate Tribal Liaison(s) to act as the ILT's representative(s) in matters pertaining to this TCP. The Tribal Liaison(s) will be at the manager level or designated representative(s) of the IAC and shall be responsible for ensuring that System of Care programs are engaging with Tribes consistent with this TCP.

The Tribal Chairperson can designate a Tribal Designee for a period of up to one year or as needed, as determined by the Tribe, and established through a resolution or letter from the Tribal Chairperson. Interactions and collaborations with Tribes are important; however, they do not constitute Tribal Consultation, except pursuant to and within the express terms of a tribal resolution or letter from the Chairperson designating a person or organization as a Tribal Designee to represent the Tribe in its Consultation with the ILT and/or IAC.

5. PROCESS AND PROCEDURE:

a. Outreach. The ILT and/or IAC shall consult with Tribes and make relevant information available within 10 business days, or sooner as deemed appropriate, and allow Tribes to respond and substantively engage in planning, program, regulatory, or other processes as time permits. The System of Care agencies shall make available upon request any current Tribal Consultation Policy and the name and contact information of their Tribal Liaison(s).

b. Initiating Consultation. Tribes may initiate Consultation with the ILT by contacting the ILT's Tribal Liaison(s). The ILT and/or IAC may initiate Consultation by reaching out to the Tribal Representative/Designee. The ILT and/or IAC may use the contact list of Tribal Chairpersons maintained by the Governor's Tribal Advisor website as needed, or use any other contact lists deemed appropriate for the purpose of Consultation.

c. Consultations. Consultation may be facilitated through means that include, but are not limited to one or more of the following, as appropriate to the subject of the Consultation:

i. E-mail

ii. Teleconference and/or Telephone

iii. Face-to-face meetings

iv. Roundtables

v. Mailings

vi. Other regular or special Consultation sessions

Tribal approved and constituted workgroups or taskforce efforts may be made by the parties to define and document the complexity, time constraints, and implications of the issues upon which consultation occurs. The ILT Tribal Liaison(s) will communicate and collaborate with Tribes in a manner that is timely and respectful. Internal processes and timelines will be clearly identified, and appropriate staff will be available to explain processes and timelines, as needed.

d. Timely Notice. The Parties recognize that Tribes have their own internal processes to negotiate policies and practices and/or may be located in remote regions, which necessitates adequate notice prior to Consultation or meetings. Contact with Tribes shall be initiated as early and as promptly as possible to provide sufficient time for Tribes to offer substantive input. Tribal requests for additional time to prepare for or attend a Consultation session or in-person meeting will be honored.

e. Emergency Consultation Process. Consultation typically should be conducted with advance notice, but should the Parties require Consultation with a Tribe in a state of emergency declared by the Governor, the Tribal Liaison(s) will contact the Tribal Representative/Designee immediately to provide a summary of the actions and potential impacts, provide opportunity for the Tribe to participate in an emergency Consultation, and identify mutually agreed upon terms by which the emergency Consultation will occur.

f. Funding: To the extent the Parties have access to State funding specifically allocated to support Consultation with Tribes, any such funding may be accessible to Tribes who engage in Consultation to support their travel, time, and other costs related to the Consultation process. The Parties will notify the Tribal Representative/Designee of funding availability, where applicable, when initiating Consultation.

g. Dispute Resolution: For resolution of disputes between the Parties regarding local programs, policies and practices that affect tribal communities and tribal children/families, the following shall apply:

i. Parties will attempt in good faith to resolve any dispute or disagreement arising out of this TCP within a reasonable timeframe deemed appropriate by both Parties.

ii. The Parties will seek to settle relevant disputes by focusing on the shared vision, values and practices of this TCP.

iii. Parties may elect to refer to an expert or third-party facilitator to assist with dispute resolution.

iv. Activities under this TCP shall continue during any necessary dispute proceeding or any other dispute resolution mechanism

Resolution activities will include a process and timeline to discuss and document any viable alternatives to recommendations proposed during Consultation that the Parties elect not to adopt.

h. Consultation Best Practices:

i. Make regular and ongoing efforts to identify potential areas of concern impacting Tribes and/or Indian Organizations.

ii. To the extent practicable, Parties will provide notice of any new local or Orange County related policy, regulations, rule, program, or other activity impacting Tribes and/or Indian Organizations.

iii. Initiate Consultation with letter or email correspondence requesting Consultation or providing notice to the Tribal Representative/Designee. Correspondence may include, but is not limited to, the following:

- A draft or overview of the need for the policy, rule, regulation, program or project;
- A draft or overview of the policy, rule, regulation, program or project;
- A summary describing how it may affect Tribes and/or Indian Organizations (if known);
- A contact person, timeline of the project, and any other relevant information to assist the Tribes and/or Indian Organizations to determine if Consultation is in the best interest of the Parties.

iv. Communicate with the Tribe(s) and/or Indian Organizations, beginning early in the planning process and continuing throughout the project. As warranted, develop an agreed-upon interval by which consultation will occur, to ensure the Tribe is provided opportunities for adequate, meaningful Consultation.

v. Invite Tribal and Indian Organization participation in the development of agendas for ongoing Consultation meetings.

vi. As appropriate, offer to utilize multiple venues for Consultation, acquainting parties with both County and Tribal/Indian Organization facilities.

vii. Foster a relationship between the ILT, IAC and Tribes and Indian Organizations, such as by coordinating an annual meeting regarding programs that directly impact Tribes and tribal communities.

viii. Identify facilitators for meetings, perhaps alternating between the ILT, IAC and the Tribe(s) and/or Indian Organizations, or an agreed-upon third party.

ix. Take tribal views and concerns into account, implement them in ILT actions, and work together to maximize all available resources.

6. CONSULTATION RECORD:

Any reports and related documentation produced during or following Consultation will include Consultation meeting details and topics, specific recommendations identified, and any follow-up actions taken and/or planned. Documentation from Consultation meetings will be maintained by the ILT and/or IAC and shared with all attendees. The Parties will elicit

feedback regarding Consultation meetings, agendas and minutes, including what was meaningful to inform best practices and what could be improved in future meetings.

7. ADOPTION AND AMENDMENTS:

This TCP shall become effective upon approval by the Parties, and the date of said approval shall be noted in the Title of the document. Parties may propose amendments to this TCP, but all such proposals must be in writing. Proposed amendments shall be considered for review and adoption by the ILT's executive leadership after Consultation and full consideration, in keeping with the spirit and provisions of this policy. The ILT retains the right not to agree to amendments that could impede its performance of the duties and obligations for which it is responsible under all applicable laws, regulations, and CDSS written guidance.

Approved and adopted by the County of Orange, Interagency Leadership Team Tribal Consultation Policy Workgroup:

Orange County Department of Education	Dennis Cole, Director of Educational Partnerships dcole@ocde.us (714) 245-6404 Raina Lee, Foster Youth Services Coordinator rlee@ocde.us (714) 668-7830
Orange County Health Care Agency	Alice Kim AlKim@ochca.com (714) 796-8285 Alicia Lemire ALemire@ochca.com (714) 834-5480 Dawn M. Smith, Assistant Deputy Director – Children and Youth Services DawnSmith@ochca.com (714) 834-5015
Orange County Probation Department	Jessica Johnson, Chief Deputy Probation Officer jessica.johnson@prob.ocgov.com (714) 645-7004 Ivy White, Division Director ivy.white@prob.ocgov.com (714) 896-7555
Orange County Social Services Agency	Jyothi Atluri, Division Director of Children and Family Services Jyothi.Atluri@ssa.ocgov.com

	(714) 541-7793 Emily Burgos, Procurement Contract Analyst Emily.Burgos@ssa.ocgov.com (714) 245-6271 Kristi Fiskum, Human Services Deputy Director Kristi.Fiskum@ssa.ocgov.com (714) 245-6130 Priscilla Gallardo, Indian Child Welfare Act (ICWA) Liaison Priscilla.Gallardo@ssa.ocgov.com (714) 380-8355 Martin Raya, Human Services Manager, Senior Martin.Raya@ssa.ocgov.com (714) 245-6071
Regional Center of Orange County	Jeanette Ruiz JRuiz2@rcocdd.com (714) 796-2905 Teresa Ta, Manager of Safety Net and Resource Development tta@rcocdd.com (714) 796-5192
Gabrielino/Tongva Nation	Sandonne Goad, Tribal Council Chairwoman Sgoad@gabrielino-tongva.com
Southern California Tribal Chairmen's Association, Inc., Tribal TANF Program	Salina Anderson, Case Manager SAnderson@sctca.net (714) 450-9240 Veronica Streb, Assistant Sites Director VStreb@sctca.net (714) 450-9240
Juaneño Band of Mission Indians/Acjachemen Nation	Patricia Dixon, Tribal Enrollment Officer PDixon1@verizon.net Heidi Lucero, Tribal Chairwoman JBMIAN.Chairwoman@gmail.com
Tribal STAR	Sunni Dominguez, Program Manager sadominguez@sdsu.edu
Sacred Path Indigenous Wellness Center	Dr. Carrie Johnson, Chief Executive Officer cjohnson@sacredpath.org

ATTACHMENT B
DATA SHARING PROTOCOLS
BETWEEN
THE COUNTY OF ORANGE SOCIAL SERVICES AGENCY
AND
THE COUNTY OF ORANGE HEALTH CARE AGENCY

1. PURPOSE

1.1 This Attachment B establishes the conditions under which SSA and HCA agree to disclose and receive data on mutual clients participating in SSA Child Welfare Services and HCA Behavioral Health Services, and shall:

1.1.1 Provide for the protection of that data;

1.1.2 Identify the responsibilities of each party; and

1.1.3 Establish terms governing the use, disclosure and disposition of the data.

1.2 This Attachment B is not intended nor designed to mandate or require a specific technology, create a single entity that exchanges information, or create a single repository of data.

1.3 Data sharing between SSA and HCA will assist to determine how many child welfare services parents and youth with mental health and/or substance use vulnerabilities are accessing behavioral health services administered by HCA and what their behavioral health services outcomes are.

1.4 This Attachment B shall apply to SSA and HCA only, and no other Party to this MOU shall be bound thereby.

2. DEFINITIONS

2.1 Data: Any and all information received, stored, processed, generated, used, transferred, disclosed, made accessible, or shared pursuant to this Attachment B, including, but not limited to, data elements, information related to the provision of mental health and substance use disorder services, and child welfare services. Data may include, but not be limited to the following data elements:

2.1.1 *Anonymized Data.* Data which has had personally identifiable information and protected health information removed, so that the people whom the data describe remain anonymous.

2.1.2 *Deidentified Data.* Data which has had personally identifiable information (PII) and protected health information (PHI) removed, to prevent people whom the data describe from being directly or indirectly identified.

2.1.3 *Metadata*. A set of data that describes and gives information about other data.

2.1.4 *Pseudonymized Data*. Data which has had personally identifiable information and protected health information replaced with a pseudonym so that the people whom the data describe cannot be directly identified.

2.2 Data Sender: The party that is disclosing data.

2.3 Data Receiver: The party that is collecting or receiving data from the Data Sender.

2.4 Health Insurance Portability and Accountability Act (HIPAA): The standards for privacy of individually identifiable health information, the security standards for the protection of electronic protected health information and the breach notification rule (45 C.F.R. §§ 160 and 164) promulgated by the U.S. Department of Health and Human Services under the HIPAA of 1996, as in effect on the Effective Date and as may be amended, modified, or renumbered.

2.5 Personally Identifiable Information (PII): Refers to "personally identifiable information" as set forth in the California Civil Code, Section 1798.140(o).

2.6 Protected Health Information (PHI): Refers to "protected health information" as set forth in 45 C.F.R. § 160.103 of the HIPAA Regulations and "medical information" as set forth in the California Civil Code, Section 56.05(n). 42 CFR, The Part 2 statute (42 U.S.C. 290dd-2) protects "records of the identity, diagnosis, prognosis, or treatment of any patient which are maintained in connection with the performance of any program or activity relating to substance use disorder education, prevention, training, treatment, rehabilitation, or research, which is conducted, regulated, or directly or indirectly assisted by any department or agency of the United States." Confidentiality protections help address concerns that discrimination and fear of prosecution deter people from entering treatment for substance use disorder (SUD).

3. PERSONALLY IDENTIFIABLE INFORMATION

Any use or disclosure of PHI or PII pursuant to this Attachment B will be limited to the minimum PHI or PII necessary to achieve the purpose for which the information is shared and as authorized by law, under HIPAA § 164.502(b) & CMIA, except where limiting such use or disclosure to the minimum necessary is not feasible, is not required under the HIPAA Regulations, such as for treatment, payment and operations (TPO) or any other applicable law, or, is a disclosure required by applicable law. Federal regulation 42 CFR Part 2 permits the use and disclosure of Part 2 (SUD) records based on a single written patient consent form obtained one-time for all future uses and disclosures for treatment, payment, and health care operations.

4. PRIVACY AND SECURITY

SSA and HCA shall:

4.1 Fully comply with all applicable laws relating to this Attachment B and the use of shared information between parties. HCA as a hybrid Covered Entity is governed by various privacy and security regulations which include; HIPAA, 42 CFR Part 2 (SUD), and HITECH.

4.2 Maintain a secure environment that protects the exchange of PHI and/or PII in any form or format.

4.3 Utilize appropriate tools, resources and technical assistance to ensure the privacy and security of all shared information between SSA and HCA.

5. SHARED PARTY RESPONSIBILITIES

5.1 Data Sender shall:

5.1.1 Use reasonable efforts to ensure the accuracy, completeness, and timeliness of the data provided. However, Data Sender cannot guarantee data accuracy and will therefore not be held responsible for any discrepancy to Data Receiver resulting from the disclosure or use of data that is inaccurate, incomplete, or outdated.

5.1.2 Reserve the right to schedule the time and duration of the availability of electronic access to the data. Data Sender does not guarantee continuous availability during scheduled times, but will use reasonable efforts to make the data available as agreed under the recurring specified time period.

5.1.3 Provide Data Receiver with access to the data consistent with applicable laws, regulations, rules and terms and conditions of this Attachment B.

5.1.4 At the time of transmission, ensure the information provided is an accurate representation of the data contained in, or available through, its system; is sent from a system that employs security controls that meet industry standards so that the information being transmitted is intended to be free from malicious software; and is provided in a timely manner.

5.1.5 Ensure the data is sent encrypted/secure and in compliance with agency Process & Policies.

5.2 Data Receiver shall:

5.2.1 Establish and use appropriate administrative, technical, and physical safeguards to protect the data from being accessed, used, disclosed, or stored in a manner other than as provided in this Attachment B. Written protocols shall be provided to Data Receiver upon request.

5.3 Both SSA and HCA are Data Senders and Data Receivers, meaning each party is responsible for securely transmitting and receiving information as part of a

bi-directional data-sharing process.

6. DATA SHARING

6.1 On a mutually agreed upon recurring basis, SSA will provide HCA with a subset of identifying data on child welfare services parents and youth through secure email or another agreed upon secure data transferring method, for a specified time period to identify mutual clients participating in HCA Behavioral Health Services.

6.2 SSA will provide a subset of client level data, including, but not limited to:

6.2.1 Client data (e.g., age, date of birth, gender, ethnicity).

6.2.2 Case data (e.g., start date, end date, case service component).

6.2.3 Referral data (e.g., reason for removal).

6.2.4 Foster care placement data (e.g., placement type, time in placement).

6.2.5 Substance use disorder related data (e.g., infant exposure to substances, referral to services, service completion, service outcomes).

6.2.6 Mental Health related data (e.g., diagnosis and medication).

6.2.7 Foster care outcomes data (e.g., reunification, placement stability).

6.2.8 Plan of Safe Care data (e.g., plan developed, referral made to services).

6.3 On a mutually agreed upon recurring basis, HCA will provide SSA with aggregate non-identifying data through a secured method on child welfare services parents and youth who have participated in, or are currently participating in, HCA Behavioral Health Services during the specified time period describing the mutual clients' mental health and substance use service outcomes. Data may be correlated to their child welfare services outcomes, where possible.

6.4 HCA will provide SSA with aggregated data, as incorporated herein by reference, and as updated over time. If the data set is too small to ensure de-identification or could lead to the identification of an individual, HCA may be unable to report that information. Aggregated data may include:

6.4.1 Age Groups.

6.4.2 Race/Ethnicity Groups.

6.4.3 Primary Diagnosis Categories.

6.4.4 Secondary Diagnosis Categories.

6.4.5 Types of Services provided.

6.5 Identifying data and non-identifying data may include Anonymized Data, Deidentified Data, Metadata and Pseudonymized Data. HCA shall be responsible for verifying and ensuring the data provided cannot be re-identified.

7. COLLABORATION WITH THE INTERAGENCY LEADERSHIP TEAM

SSA and HCA shall collaborate in good faith with the Interagency Leadership Team (ILT) to implement the provisions of this Attachment B, including, but not limited to:

7.1 Providing non-privileged data as reasonably requested; and

7.2 Providing assistance and other applicable requested data to the ILT for the purposes of performing activities related to this Attachment B.

ATTACHMENT C

COUNTY OF ORANGE INFORMATION TECHNOLOGY SECURITY PROVISIONS

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

    a) **Contractor System(s) and Security:** At all times during the contract term, Contractor shall maintain a level of security with regard to the Contractor Systems, that in all

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

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

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

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

8. Security Breach Notification: In the event Contractor becomes aware of any act, error or omission, negligence, misconduct, or security incident including unsecure or improper data disposal, theft, loss, unauthorized use and disclosure or access, that compromises or is suspected to compromise the security, availability, confidentiality, and/or integrity of County data or the physical, technical, administrative, or organizational safeguards required under this Contract that relate to the security, availability, confidentiality, and/or integrity of County data, Contractor shall, at its own expense, (1) immediately (or within 24 hours of potential or suspected breach), notify the County's Chief Information Security Officer and County Privacy Officer of such occurrence; (2) perform a root cause analysis of the actual, potential, or suspected breach; (3) provide a remediation plan that is acceptable to County within 30 days of verified breach, to address the occurrence of the breach and prevent any further incidents; (4) conduct a forensic investigation to determine what systems, data, and information have been affected by such event; and (5) cooperate with County and any law enforcement or regulatory officials investigating such occurrence, including but not limited to making available all relevant records, forensics, investigative evidence, logs, files, data reporting, and

other materials required to comply with applicable law or as otherwise required by County and/or any law enforcement or regulatory officials, and (6) perform or take any other actions required to comply with applicable law as a result of the occurrence (at the direction of County).

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

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

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

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

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

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

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

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

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

10. Business Continuity and Disaster Recovery (BCDR):

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

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

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

ATTACHMENT D

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.

8. Inactivity Timeout and Restricted Connection Times

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

b. 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.

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

9. Account Monitoring

a. 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.)

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

c. 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.

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

e. 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.

10. Administrative Privileges

a. 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.

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

c. 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.

d. 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.

e. 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.

f. All passwords for privileged system-level accounts (e.g., root, enable, OS admin, application administration accounts, etc.) shall comply with Controls Management B.7.

11. Remote Access

a. 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.

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

c. 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.

d. Remote sessions shall be terminated after 15 minutes of inactivity requiring the user to authenticate again to access County resources.

e. All remote access infrastructures shall include the capability to monitor and record a detailed audit trail of each remote access attempt.

f. 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.

g. Periodic assessments shall be performed to identify unauthorized remote connections. Results shall be used to address any vulnerabilities and prioritized according to criticality.

h. 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.

i. Users attempting to use external remote access shall utilize a County-approved multi-factor authentication process.

j. 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.

k. 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.

12. Wireless Access

a. 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.

b. Only wireless systems that have been evaluated for security by both department management and the County shall be approved for connectivity to County networks.

c. County data that is transmitted over any wireless network shall be protected in accordance with the sensitivity of the information.

d. 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.

e. 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.

13. System and Network Operations Management

a. Operating procedures and responsibilities for all County information processing facilities shall be formally authorized, documented, and updated.

b. Departments and/or contractors shall establish controls to ensure the security of the information systems networks that they operate.

c. Operational system documentation for County information systems shall be protected from unauthorized access.

d. System utilities shall be available to only those users who have a business case for accessing the specific utility.

14. System Monitoring and Logging

a. Systems operational staff shall maintain appropriate log(s) of activities, exceptions and information security events involving County information systems and services.

b. Each department and/or contractor shall maintain a log of all faults involving County information systems and services.

c. Logs shall be protected from unauthorized access or modifications wherever they reside.

d. 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.

e. Auditing and logging of user activity shall be implemented on all critical County systems that support user access capabilities.

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

15. Malware Defenses

a. 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.

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

c. 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.

16. Data Loss Prevention

a. Departments and/or contractor shall implement host-based Data Loss Prevention (DLP) to reduce the risk of data breach related to sensitive information.

b. Departments and/or contractors shall deploy encryption software on mobile devices containing sensitive.

17. Data Transfer

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

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

18. Encryption

a. 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.

b. 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.

c. Where appropriate, encryption shall be used to protect confidential application data that is transmitted over open, untrusted networks, such as the Internet.

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

e. Determination of the level of cryptographic controls

f. Key management/distribution steps and responsibilities

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

19. System Acquisition and Development

a. 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.

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

c. 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.

d. 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.

e. 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.

20. Business Requirements

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

21. System Files

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

b. 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.

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

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

e. 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.

22. System Development & Maintenance

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

b. 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.

c. 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.

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

e. 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.

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

g. Departments and/or contractors are responsible for managing outsourced software development related to department-owned IT systems.

23. System Requirements

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.

24. Procurement Controls

a. Breach notification requirements clause to be included in new or renewal contracts for systems containing sensitive information.

b. 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.

c. 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:

i. SOC 1 Type 2

ii. SOC 2 Type 2

iii. Security Certifications (ISO, PCI, etc.)

iv. FedRAMP certification

v. Penetration Test Results

25. IT Services Provided to Public

a. 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.

26. Removable Media

a. 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.