County of Los Angeles
DEPARTMENT OF PUBLIC SOCIAL SERVICES
12860 CROSSROADS PARKWAY SOUTH · CITY OF INDUSTRY, CALIFORNIA 91746
(562) 908-8400 · dpss.lacounty.gov

JACKIE CONTRERAS, Ph.D.
Director

MICHAEL J. SYLVESTER II
Chief Deputy Director, Administration

KRISTIN STRANGER
Chief Deputy Director, Operations

July 29, 2025

The Honorable Board of Supervisors
County of Los Angeles
383 Kenneth Hahn Hall of Administration
500 West Temple Street
Los Angeles, California 90012

Dear Supervisors:

RECOMMENDATION TO AWARD A MASTER AGREEMENT TO VARIOUS AGENCIES TO PROVIDE COMMUNITY SERVICES BLOCK GRANT PROGRAM SERVICES (ALL DISTRICTS - 3 VOTES)

SUBJECT

The Department of Public Social Services (DPSS) seeks approval to execute Master Agreements (MAs) with 54 community-based and faith-based organizations, and public entities for the provision of the Community Services Block Grant (CSBG) program services for a three-year term, effective January 1, 2026 through December 31, 2028, with an option to extend for up to two additional one-year periods. The approval of the MAs will allow DPSS to partner with community-based and faith-based organizations, and public entities to provide a variety of services to low-income families and individuals throughout the County of Los Angeles Community Action Agency (CAA) service area.

IT IS RECOMMENDED THAT THE BOARD:

1. Delegate authority to the Director of DPSS, or their designee, to prepare and execute MAs with the 54 organizations listed on Enclosure I, in substantially similar form as Enclosure II, effective January 1, 2026 through December 31, 2028. The Director of DPSS, or their designee, will notify the Board within ten business days after execution.

2. Delegate authority to the Director of DPSS, or their designee, to prepare and execute amendments to extend the MA for two additional one-year periods, for a maximum contract term of five years. The approval of County Counsel as to form will be obtained prior to executing such amendments. The Director of DPSS, or their designee, will notify the Board within ten business days after executing such amendments.

3. Delegate authority to the Director of DPSS, or their designee, to award CSBG MAs to additional agencies during the three-year period, and any extension periods, provided that: a) Such agencies meet all of the minimum mandatory requirements outlined in the initial Request for Statement of Qualifications (RFSQ) dated October 10, 2024; b) There is a need for the Core Service Category(ies) in the Supervisorial District(s) for which agencies apply; and c) The Director of DPSS, or their designee, will notify the Board in writing within ten business days after execution.

4. Delegate authority to the Director of DPSS, or their designee, to award Service Requisitions (SR) for CSBG program services to agencies with MAs as needed. The Director of DPSS, or their designee, will notify the Board within ten business days after execution. The total cost for services under the SRs is to be determined based on annual federal CSBG allocations. The estimated annual cost for subsequent Fiscal Years (FYs) will be included in DPSS' budget requests.

5. Delegate authority to the Director of DPSS, or their designee, to prepare and execute amendments to the MAs and/or Service Requisitions for: a) Instances which affect the scope of work, contract term, contract sum, payment terms, or any other term or condition; b) Additions and/or changes required by the Board or Chief Executive Office (CEO); c) Changes to be in compliance with applicable federal, State, and County regulations; or d) Increases or decreases to the SR amounts based on contractor's performance, community needs, and funding availability. The approval of County Counsel as to form will be obtained prior to executing such amendments. The Director of DPSS, or their designee, will notify the Board within ten business days of executing such amendments.

6. Delegate authority to the Director of DPSS, or their designee, to suspend or terminate CSBG MAs and/or SRs on behalf of the County in accordance with the applicable provisions in the respective Agreements. The approval of County Counsel as to form will be obtained prior to executing suspensions or terminations. The Director of DPSS, or their designee, will notify the Board at least ten days in advance of executing terminations.

PURPOSE/JUSTIFICATION OF RECOMMENDED ACTION

The recommended actions will allow DPSS to create a pool of qualified community-based and faith-based organizations and public entities to provide CSBG program services to assist low-income individuals and families attain the skills, knowledge, and motivation necessary to achieve self-sufficiency throughout the County of Los Angeles CAA service area.

Implementation of Strategic Plan Goals

The recommended actions support and are consistent with the Countywide Strategic Plan, North Star I – Make Investments that Transform Lives, Focus Area Goal B – Employment and Sustainable Wages via Strategies i, ii, and iv, and Focus Area Goal D – Support Vulnerable Populations via Strategies vii, viii, and ix; and North Star II – Foster Vibrant and Resilient Communities, Focus Area Goal E – Economic Health via Strategies i and iv, and Focus Area Goal F – Community Connections via Strategy iii.

FISCAL IMPACT/FINANCING

The estimated cost of the SR for Calendar Years 2026-2028, and extension periods, will be determined based on federal allocations. The Calendar Year 2025 allocation was $6,270,685. The

funding for CSBG services is included in DPSS' FY 2025-26 Budget Request and will be included in the Department's budget requests for subsequent FYs. CSBG program services are fully funded by federal appropriations through the California Department of Community Services and Development, and there is no impact on Net County Cost.

DPSS will fund all services within its approved budget for the CSBG services. DPSS will confirm that funding is available before SR are executed.

FACTS AND PROVISIONS/LEGAL REQUIREMENTS

The purpose of the CSBG program is to assist low-income families and individuals achieve economic self-sufficiency through a variety of services such as employment, senior and/or disabled adult, emergency, legal, domestic violence, and child and family development services.

The County of Los Angeles CAA service area includes all the cities and unincorporated areas of the County except the cities of Arcadia, Duarte, Los Angeles, Long Beach, Monrovia, Pasadena, Sierra Madre, South Pasadena, and the unincorporated area of Altadena. In order to receive CSBG services, participants must be at or below 200 percent of the federal poverty level and reside within the CAA service area. Funding for CSBG services is allocated among the five Supervisorial Districts based on the percentage of low-income individuals in the CAA service area that reside in each District (Enclosure III). The allocation is based on 2020 census data and on the Los Angeles County Supervisorial District boundaries that were re-drawn in 2021.

County Counsel reviewed this Board letter and approved the MA (Enclosure II) as to form. The MA will not result in the unauthorized disclosure of confidential information and will be in full compliance with federal, State, and County regulations and requirements.

All contractors, current and prospective, are, and will be, in compliance with all Board, CEO, and County Counsel requirements.

CONTRACTING PROCESS

On October 10, 2024, DPSS released an RFSQ for CSBG Program services. The RFSQ was advertised on DPSS' social media platforms, the CEO's The Way Home Newsletter, and in the following newspapers: Los Angeles Times, La Opinion, Long Beach Press Telegram, Antelope Valley Press, and the San Gabriel Valley Tribune. The RFSQ was also posted on the County of Los Angeles Solicitations and DPSS' Contract Opportunities websites.

DPSS received Statement of Qualifications (SOQs) from 59 agencies. A total of five agencies were disqualified for failing to meet the minimum mandatory requirements. Of the 59 agencies that responded to the CSBG RFSQ, the Department recommends entering into MAs with 54 qualified agencies (Enclosure I). With the Board's approval, DPSS will continue to accept and evaluate SOQs from additional agencies throughout the term of the MA. Such agencies may be awarded an MA if they meet the initial RFSQ requirements. Information about the MA, the RFSQ requirements, and the opportunity to submit SOQs is posted on the County's website.

REQUEST FOR SERVICES AND SERVICE REQUISITION PROCESS

DPSS will work with the Supervisorial District Offices to determine which Core Service Categories and Subservices are to be funded based on the service needs and funding priorities of the five

Supervisorial Districts. DPSS will identify the MA agencies that are qualified to provide the needed Core Service Categories and Subservices in the Districts and then send a Request for Services (RFS) to such agencies. The RFS will include a Statement of Work for the Core Service Category and if applicable, Subservice(s).

In response to the RFS, interested MA agencies will submit proposals to DPSS including a detailed work plan, measurable outcomes, a budget, a fixed cost for each service, and proof of insurance. SRs will be issued to those MA agencies selected from the RFS process. Additional services not included in the Service Requisition will require an amendment to the SR.

IMPACT ON CURRENT SERVICES (OR PROJECTS)

Approval of the recommended actions will enable DPSS to continue to provide CSBG Program services to low-income individuals and families throughout the County of Los Angeles CAA service area without interruption.

The recommended actions will not infringe on the role of the County in relationship to its residents, and the County's ability to respond to emergencies will not be impaired. There is no change in risk exposure to the County.

CONCLUSION

Upon Board approval, the Executive Office of the Board of Supervisors is requested to return one adopted stamped Board letter to DPSS.

Respectfully submitted,

JACKIE CONTRERAS, Ph.D.
Director

JC:lv

Enclosures

c: Chief Executive Office
Executive Office, Board of Supervisors
County Counsel

RECOMMENDED AGENCIES 2026-2028

SUPERVISORIAL DISTRICT 1

	Agency Name	Core Service(s)					
		Child and Family Development Services	Domestic Violence Services	Emergency Services	Employment Services	Legal Services	Senior and/or Disabled Adult Services
1	1736 Family Crisis Center		X				
2	Asian Youth Center	X		X	X		
3	Boys & Girls Club of West San Gabriel Valley	X					
4	Catholic Charities of Los Angeles, Inc.			X	X		
5	Chinatown Service Center				X		X
6	Clothes The Deal				X		
7	Crossroads, Inc.			X			
8	Eastmont Community Center	X		X			X
9	Harriett Buhai Center for Family Law		X			X	
10	Helpline Youth Counseling, Inc.	X	X	X			
11	Hillsides	X			X		
12	Inland Valley Council of Churches			X			
13	Jovenes, Inc.			X			
14	Los Angeles Center for Law and Justice, Inc.					X	
15	LTSC Community Development Corporation						X
16	Neighborhood Legal Services of Los Angeles County		X			X	
17	Soledad Enrichment Action	X					
18	The Rector, Wardens and Vestry of the Church of Our Saviour, in San Gabriel, California			X			
19	UAW-Labor Employment and Training Corporation				X		
20	Young Men's Christian Association of Metropolitan Los Angeles	X					X
21	YWCA of San Gabriel Valley		X	X			X

RECOMMENDED AGENCIES 2026-2028

SUPERVISORIAL DISTRICT 2

	Agency Name	Core Service(s)					
		Child and Family Development Services	Domestic Violence Services	Emergency Services	Employment Services	Legal Services	Senior and/or Disabled Adult Services
1	1736 Family Crisis Center		X	X			
2	Asian American Drug Abuse Program, Inc.	X			X		
3	Asian Youth Center	X		X	X		
4	Beach Cities Health District	X					X
5	Boys & Girls Clubs of Metro Los Angeles	X					
6	Boys' and Girls' Club of Santa Monica, Inc.	X					
7	Catholic Charities of Los Angeles, Inc.		X		X		
8	Clothes The Deal				X		
9	Coalition for Responsible Community Development			X	X		
10	Community Legal Aid SoCal					X	
11	Didi Hirsch Psychiatric Service	X					
12	Harriett Buhai Center for Family Law		X			X	
13	Jenesse Center, Inc.		X	X		X	
14	LTSC Community Development Corporation						X
15	New Star Family Center		X				
16	Office of Samoan Affairs of California, Inc.	X	X	X	X		X
17	PATH			X	X		
18	Peace4Kids	X					
19	Personal Involvement Center, Inc.	X	X				
20	SHIELDS For Families	X		X	X		
21	Soledad Enrichment Action	X					
22	The Richstone Center, Inc.	X	X				
23	UAW-Labor Employment and Training Corporation				X		
24	Upward Bound House			X			
25	Young Men's Christian Association of Metropolitan Los Angeles	X					X

RECOMMENDED AGENCIES 2026-2028

SUPERVISORIAL DISTRICT 3

	Agency Name	Core Service(s)					
		Child and Family Development Services	Domestic Violence Services	Emergency Services	Employment Services	Legal Services	Senior and/or Disabled Adult Services
1	1736 Family Crisis Center		X				
2	Asian Youth Center	X		X	X		
3	Boys' and Girls' Club of Santa Monica, Inc.	X					
4	Clothes The Deal				X		
5	Covenant House California			X			
6	Didi Hirsch Psychiatric Service	X					
7	Haven Hills, Inc.		X				
8	Neighborhood Legal Services of Los Angeles County		X			X	
9	UAW-Labor Employment and Training Corporation				X		
10	Upward Bound House			X			
11	Young Men's Christian Association of Metropolitan Los Angeles	X					X

RECOMMENDED AGENCIES 2026-2028

SUPERVISORIAL DISTRICT 4

	Agency Name	Core Service(s)					
		Child and Family Development Services	Domestic Violence Services	Emergency Services	Employment Services	Legal Services	Senior and/or Disabled Adult Services
1	1736 Family Crisis Center		X	X			X
2	Asian Youth Center	X		X	X		
3	Beach Cities Health District	X					
4	Boys and Girls Club of Whittier, Inc.	X					
5	Boys & Girls Clubs of Metro Los Angeles	X					
6	Catholic Charities of Los Angeles, Inc.			X			
7	Clothes The Deal				X		
8	Coalition for Responsible Community Development			X			
9	Community Legal Aid SoCal					X	
10	Harriett Buhai Center for Family Law		X			X	
11	Helpline Youth Counseling, Inc.	X	X	X			
12	Hillsides	X			X		
13	Jovenes, Inc.			X			
14	Los Angeles Center for Law and Justice, Inc.					X	
15	LTSC Community Development Corporation						X
16	Niswa Association, Inc.		X				
17	Office of Samoan Affairs of California, Inc.	X	X	X	X		X
18	PATH			X	X		
19	Project IMPACT Inc.	X					
20	Soledad Enrichment Action	X					
21	South Asian Helpline and Referral Agency		X				X
22	Su Casa ~ Ending Domestic Violence		X				
23	UAW-Labor Employment and Training Corporation				X		
24	Women's and Children's Crisis Shelter, Inc.		X				
25	Young Men's Christian Association of Metropolitan Los Angeles	X					X

RECOMMENDED AGENCIES 2026-2028

SUPERVISORIAL DISTRICT 5

	Agency Name	Core Service(s)					
		Child and Family Development Services	Domestic Violence Services	Emergency Services	Employment Services	Legal Services	Senior and/or Disabled Adult Services
1	Antelope Valley Domestic Violence Council	X	X	X		X	
2	Armenian Relief Society of Western USA, Inc.				X		X
3	Asian Youth Center	X		X	X		
4	Catholic Charities of Los Angeles, Inc.				X		
5	Chinatown Service Center				X		X
6	Clothes The Deal				X		
7	Didi Hirsch Psychiatric Service	X					
8	Friends Outside in Los Angeles County				X		
9	Home Again Los Angeles			X			
10	LTSC Community Development Corporation						X
11	Neighborhood Legal Services of Los Angeles County		X			X	
12	Optimist Boys' Home and Ranch	X					
13	Personal Involvement Center, Inc.	X	X				
14	Santa Clarita Valley Boys' and Girls' Club	X					
15	Soledad Enrichment Action	X					
16	The Antelope Valley Boys and Girls Club	X					
17	The Boys & Girls Club of Burbank and Greater East Valley, Inc.	X					
18	UAW-Labor Employment and Training Corporation				X		
19	Young Men's Christian Association of Metropolitan Los Angeles	X					X
20	YWCA of Glendale and Pasadena		X			X	
21	YWCA of San Gabriel Valley		X				X

ENCLOSURE II

SAMPLE

MASTER AGREEMENT

BY AND BETWEEN

COUNTY OF LOS ANGELES

DEPARTMENT OF PUBLIC SOCIAL SERVICES

AND

(CONTRACTOR)

FOR

COMMUNITY SERVICES BLOCK GRANT PROGRAM

SERVICES

SAMPLE MASTER AGREEMENT
TABLE OF CONTENTS

SAMPLE MASTER AGREEMENT
TABLE OF CONTENTS

SAMPLE MASTER AGREEMENT
TABLE OF CONTENTS

SAMPLE MASTER AGREEMENT
TABLE OF CONTENTS

SAMPLE MASTER AGREEMENT
TABLE OF CONTENTS

STANDARD EXHIBITS

SAMPLE MASTER AGREEMENT BETWEEN
COUNTY OF LOS ANGELES,
DEPARTMENT OF PUBLIC SOCIAL SERVICES
AND
(CONTRACTOR)
FOR
COMMUNITY SERVICES BLOCK GRANT PROGRAM SERVICES

This Master Agreement and Exhibits made and entered into on _____ ("Execution Date") by and between the County of Los Angeles, Department of Public Social Services hereinafter referred to as "County" and _____, hereinafter referred to as "Contractor" to provide Community Services Block Grant (CSBG) Program services.

RECITALS

WHEREAS, the County may contract with public entities and private non-profit community-based and faith-based organizations for CSBG Program Services when certain requirements are met; and

WHEREAS, the Contractor is a public entity or private non-profit community-based or faith-based organization; and

WHEREAS, this Master Agreement is therefore authorized under the CSBG Grant Act, 42 USC 9901 and the California CSBG Program, California Codes, Government Code Section 12725 et seq.; and

WHEREAS, the Board of Supervisors has authorized the Director of the Department of Public Social Services (DPSS) or designee to execute and administer this Master Agreement; and

NOW THEREFORE, in consideration of the mutual covenants contained herein, and for good and valuable consideration, the parties agree to the following:

1.0 APPLICABLE DOCUMENTS

Exhibits A through O are attached to and form a part of this Master Agreement. In the event of any conflict or inconsistency in the definition or interpretation of any word, responsibility, schedule, or the contents or description of any task, deliverable, goods, service, or other work, or otherwise between the base Master Agreement and the Exhibits, or between Exhibits, such conflict or inconsistency will be resolved by giving precedence first to the Master Agreement and then to the Exhibits according to the aforementioned list referenced in the Table of Contents.

This Master Agreement and the Exhibits hereto constitute the complete and exclusive statement of understanding between the parties, and supersedes all previous Master Agreements, written and oral, and all communications between the parties relating to the subject matter of this Master Agreement. No change to this Master Agreement will be valid unless prepared pursuant to Subsection 8.1 (Amendments and Change Notices) and signed by both parties.

2.0 DEFINITIONS

Standard Definitions

The headings herein contained are for convenience and reference only and are not intended to define the scope of any provision thereof. The following words as used herein will be construed to have the following meaning, unless otherwise apparent from the context in which they are used.

2.1 **Board of Supervisors**: The Board of Supervisors is the governing body for the County of Los Angeles (County).

2.2 **Budget**: The document that details the Contractor's projected costs for providing services and is included in the Service Requisition.

2.3 **Business Day(s)**: Monday through Friday between the hours of 8:00 A.M. to 5:00 P.M., excluding County Holidays.

2.4 **Calendar Day(s)**: All days of the week including Saturdays, Sundays, and Holidays.

2.5 **Calendar Year (CY)**: The twelve (12) month period beginning January 1st and ending the following December 31st.

2.6 **Community Services Block Grant (CSBG)**: The CSBG Program is designed to provide a range of services to assist low-income individuals and families attain the skills, knowledge and motivation necessary to achieve self-sufficiency.

2.7 **Contract Discrepancy Report (CDR)**: A report used by the County Contract Administrator to record contract discrepancies or problems with Contractor's performance. If Contractor is not complying with contract requirements and/or Contractor's performance is determined to be

unsatisfactory, the County Contract Administrator is required to forward a CDR to the Contractor for its response.

2.8 **Contract Invoicing System (CIS)**: The CSBG Program's automated invoicing system. It also records and tracks State required program outcome information for reporting purposes.

2.9 **Contractor**: A Master Agreement agency who has met all requirements, and has an executed Master Agreement and Service Requisition(s).

2.10 **Contractor's Contract Manager**: The individual designated by the Contractor to administer the Master Agreement operations after the Master Agreement award.

2.11 **County Contract Administrator**: The individual designated by the County with authority to act as outlined in Section 6.0, Subsection 6.4.

2.12 **County Contract Director**: The individual designated by the County with authority to act as outlined in Section 6.0, Subsection 6.2.

2.13 **County Contract Program Manager**: The individual designated by County with authority to act as outlined in Section 6.0, Subsection 6.5.

2.14 **County Contract Program Monitor (CPM)**: The individual designated by the County with authority to act as outlined in Section 6.0, Subsection 6.6.

2.15 **Day(s)**: Calendar day(s) unless otherwise specified.

2.16 **DPSS Director**: Director of the Department of Public Social Services, County of Los Angeles, or their designee.

2.17 **Department of Public Social Services (DPSS)**: The County of Los Angeles Department of Public Social Services, which is entering into this Master Agreement on behalf of the County of Los Angeles. DPSS is responsible for providing financial and social services to eligible persons in the County of Los Angeles and which serves as the Los Angeles County Community Action Agency and administers the CSBG program.

2.18 **Fiscal Year**: The twelve (12) month period beginning July 1st and ending the following June 30th.

2.19 **Master Agreement**: County's standard agreement executed between County and individual Contractors. It sets forth the terms and conditions for the issuance and performance of, and otherwise governs, subsequent Service Requisitions.

2.20 **Master Agreement Agency**: An agency who has submitted a Statement of Qualifications (SOQ) in response to County's Request For Statement of Qualifications (RFSQ), has met the minimum mandatory requirements listed in the RFSQ, and has an executed Master Agreement with the Department.

2.21 **Participant**: An individual or family who receive CSBG services under this Master Agreement and resulting Service Requisition(s).

2.22 **Request for Services (RFS)**: The process which the County will utilize to solicit bids from qualified Master Agreement Agencies for the provision of CSBG services, which may result in the award of Service Requisitions.

2.23 **Request for Statement of Qualifications (RFSQ)**: A solicitation based on establishing a pool of Qualified Contractors to provide services through Master Agreements.

2.24 **Service Requisition**: A subordinate agreement executed wholly within and subject to the provisions of this Master Agreement, for the performance of services as described in a Request for Services and Statement of Work. No work will be performed by Contractors except in accordance with executed Service Requisitions.

2.25 **Standard**: A minimum requirement set by the County for the Contractor to perform a service or activity.

2.26 **Statement of Qualifications (SOQ)**: A Contractor's response to an RFSQ.

2.27 **Statement of Work**: A written description of services and/or deliverables desired by County for a specific Service Requisition.

2.28 **Supervising County Contract Administrator**: The individual designated by the County with authority to act as outlined in Section 6.0, Subsection 6.3.

2.29 **Supervisorial District**: Los Angeles County is divided into five (5) geographical areas, each with an elected Supervisor who is a member of the County of Los Angeles, Board of Supervisors.

2.30 **Unspent Funds**: What DPSS paid minus what it actually cost Contractor to provide the services.

3.0 WORK

3.1 Pursuant to the provisions of this Master Agreement, the Contractor must fully perform, complete and deliver on time, all tasks, deliverables, services and other work as set forth herein.

3.2 CSBG services that will be solicited under this Master Agreement include programs under the following six (6) Core Service Categories: Child and Family Development Services, Domestic Violence Services, Emergency Services, Employment Services, Legal Services, and Senior and/or Disabled Adult Services. Contractor is pre-qualified for the Core Service Categories in the Supervisorial Districts indicated in Exhibit A, Scope of Services. Each Service Requisition will include an attached Statement of Work, which will describe in detail the particular services and the specifications required for the performance thereof. Payment for all work will be on a fixed priced per service basis, subject to the Total Maximum Amount specified on each individual Service Requisition.

3.3 If Contractor provides any task, deliverable, service, or other work to County that utilizes other than approved Contractor Personnel, and/or that goes beyond the Service Requisition expiration date, and/or that exceeds the Total Maximum Amount as specified in the Service Requisition as originally written or modified in accordance with Subsection 8.1 (Amendments and Change Notices), these will be gratuitous efforts on the part of Contractor for which Contractor will have no claim whatsoever against County.

3.4 County procedures for issuing and executing Service Requisitions are as set forth in Subsections 3.4 and 3.5. Upon determination by County to issue a Request for Services, County will issue a Request for Services containing a Statement of Work to all Master Agreement Agencies prequalified for the applicable Core Services and Subservice(s) in the applicable Supervisorial District. Each interested Master Agreement Agency so contacted must submit a bid to DPSS within the timeframe specified in the Request for Services. Failure of Contractor to provide a bid within the specified timeframe may disqualify Contractor for that Service Requisition.

3.5 Upon completion of evaluations, County will execute the Service Requisition by and through DPSS according to the Request for Services bid evaluation criteria. It is understood by Contractor that County's competitive bidding procedure may have the effect that no Service Requisitions are awarded to some Master Agreement Agencies. Upon expiration of a Service Requisition, County may either issue a Request for Services or extend the Service Requisition beyond the calendar year, if it is in the best interest of the County.

3.6 County estimates that selection of any Contractor will occur within sixty (60) days of completion of the evaluations of the Service Requisition bids. Following selection, all Contractors selected must be available to start work on the starting date specified in the Service Requisition. Inability of Contractor to comply with such commencement date may be cause for disqualification of Contractor from the Service Requisition as determined in the sole discretion of the County.

3.7 County may issue Service Requisitions without a Request for Services process directly to a Master Agreement Agency when it is in the best interest of the County, or when all qualified Master Agreement Agencies for a particular Core Service or Subservice meet the targeted service priorities of the Supervisorial District.

3.8 In the event Contractor defaults three times under Subsection 3.6 within a given calendar year, then County may terminate this Master Agreement pursuant to Subsection 8.42 (Termination for Default).

4.0 TERM OF MASTER AGREEMENT

4.1 This Master Agreement is effective January 1, 2026, or upon the date of its execution by Director or their designee as authorized by the Board of Supervisors (Board), whichever is later. This Master Agreement will expire

on December 31, 2028, unless sooner extended or terminated, in whole or in part, as provided herein.

4.2 The County will have the sole option to extend the Master Agreement term for up to two additional one-year periods, for a maximum total Master Agreement term of five years. This option will be exercised at the sole discretion of the Director of DPSS or their designee as authorized by the Board.

4.3 The County maintains a database that tracks/monitors contractor performance history. Information entered into the database may be used for a variety of purposes, including determining whether the County will exercise a Master Agreement term extension option.

4.4 Contractor must notify the Department when this Master Agreement is within six (6) months from the expiration of the term as provided for hereinabove. Upon occurrence of this event, Contractor must send written notification to the Department at the address herein provided in Exhibit B (County's Administration).

5.0 CONTRACT SUM

5.1 Total Contract Sum

Contractor will not be entitled to any payment by County under this Master Agreement except pursuant to validly executed and satisfactorily performed Service Requisitions. The contract sum will be specified at the time of each Service Requisition award. Contractor understands and acknowledges that the County's obligation is specifically conditioned upon the County receiving the annual CSBG allocation program funds from the State. In the event that the funds for any given program year are increased/decreased, the contract amount and/or terms of any or all Service Requisitions may be adjusted accordingly.

5.2 Written Approval for Reimbursement

The Contractor will not be entitled to payment or reimbursement for any tasks or services performed, nor for any incidental or administrative expenses whatsoever incurred in or incidental to performance hereunder, except as specified herein or in an executed Service Requisition. Assumption or takeover of any of the Contractor's duties, responsibilities, or obligations, or performance of same by any entity other than the Contractor, whether through assignment, subcontract, delegation, merger, buyout, or any other mechanism, with or without consideration for any reason whatsoever, will occur only with the County's express prior written approval.

5.3 No Payment for Services Provided Following Expiration/Termination of Master Agreement

Contractor will have no claim against County for payment of any money or reimbursement, of any kind whatsoever, for any service provided by Contractor after the expiration or other termination of this Master Agreement. Should Contractor receive any such payment it will immediately notify County and must immediately repay all such funds to County. Payment by County for services rendered after expiration/termination of this Master Agreement will not constitute a waiver of County's right to recover such payment from Contractor.

5.4 Notification of Seventy-Five Percent (75%) of Total Contract Sum

The Contractor must maintain a system of record keeping that will allow the Contractor to determine when it has incurred seventy-five percent (75%) of the total contract amount under each Service Requisition. Upon occurrence of this event, the Contractor must send written notification within fifteen (15) business days to DPSS at the address herein provided in Exhibit B, County's Administration.

5.5 Invoices and Payments

5.5.1 For providing the tasks, deliverables, services, and other work authorized by Service Requisitions issued pursuant to this Master Agreement, Contractor must separately invoice County for each Service Requisition on a monthly basis. The Contractor must update billing information on the CSBG Contract Invoicing System.

Contractor updates on the Contract Invoicing System must include, but are not limited to the following:

- Registering participants;
- Creating CSBG reports/invoices; and
- Adding, editing, and removing participant information or CSBG reports/invoices.

5.5.2 Payment for all work will be on a fixed price per service basis, subject to the Total Maximum Amount specified in each Service Requisition less any amounts assessed in accordance with Subsection 8.25 (Liquidated Damages).

5.5.3 All work performed by, and all invoices submitted by, Contractor pursuant to Service Requisitions issued hereunder must receive the written approval of County Contract Administrator, who will be responsible for a detailed evaluation of Contractor's performance before approval of work and/or payment of invoices is permitted. In no event will the County be liable or responsible for any payment prior to such written approval. Approval for payment will not be unreasonably withheld.

5.5.4 The Contractor must submit complete and accurate monthly invoices to the County by the 10th calendar day of the month following the month of service by electronic invoice submission on the Contract Invoicing System. In the event the Contract Invoicing System is unavailable, Contractor must submit a signed original hard copy invoice and all back-up information to:

Attention: County Contract Administrator
Department of Public Social Services
Contract Administration and Monitoring (CAM) Division – CSBG
12900 Crossroads Parkway South
City of Industry, CA 91746-3411

If the 10th falls on a Saturday, Sunday, or County holiday, the invoices will be due the next business day.

5.5.5 **Invoice Content**

The period of performance specified in Contractor's invoice(s) must coincide with the period of performance specified in the applicable Service Requisition.

Each invoice submitted by Contractor must specify:

- County Service Requisition number;
- Month and year of work being invoiced;
- Service delivery information such as Participant identifying information and the number of service units provided to each during the report period. This may include pseudo information for sensitive services such as legal and domestic violence; and
- The total billing amount of the invoice based on the payment methodology.

5.5.6 The County will review the invoice and back-up documentation and make payment adjustments (i.e., for deductions, etc.) and authorize payment of an accurate invoice as soon as possible after receipt of the Contractor's billing. The County will make a reasonable effort to effect payment to the Contractor within thirty (30) days from receipt of an invoice that is accurate and complete as to form and content.

5.5.7 The Contractor will be required to complete an electronic signature validation process in order to submit all invoices and back-up information electronically in the Contract Invoicing System. Prior to invoice submission, the Contract Invoicing System user must comply with the electronic signature procedures.

5.5.8 The Contractor will be allowed to purchase the necessary computer equipment and software needed to support the

application. The CSBG Contract Invoicing System will run on Oracle Application Express (APEX-23) later versions; recommended browsers include Microsoft Edge and Google Chrome.

5.5.9 Withholding of Payment

Payments to the Contractor will be made monthly provided that the Contractor has submitted a complete and accurate invoice and is not in default under any provision of the Master Agreement and Service Requisition. If Contractor fails to submit accurate, complete, and timely invoices to include but not limited to the back-up documentation stated in Paragraph 5.5.6 above, the County may withhold payment to Contractor up to the full amount of any invoice that would otherwise be due, until Contractor has satisfied the concerns of the County. Approval of payment will not be unreasonably withheld.

5.5.10 Allegations of Fraud and/or Abuse

In the event of allegations of fraud or abuse (fraud and abuse as defined in appropriate Program provisions and regulations), the County reserves the right to withhold up to twenty (20) percent of the Contract amount, or the amount in dispute, or the amount of the final request for payment, whichever is greater, on a completed program until a determination is issued in writing by the Director or its representative that withheld funds should be released to the Contractor. Such written determination will not supersede or replace the final report.

5.5.11 Disallowed Costs

The County may withhold payments if the Contractor has failed to refund unexpended funds or funds spent for disallowed costs relating any DPSS contract that the Contractor has with the County. The County will require the Contractor pay and the Contractor agrees to pay the full amount of the Contractor liability to the County or the State for such audit exceptions as were caused by the Contractor, upon demand by the County at any time after completion of the grievance procedures at the Contractor level. The County will notify the Contractor of any disallowed costs.

5.5.12 Delay of Payment

The County may delay the last payment due (plus the previous full-month payment due if the last payment is for less than a full-month) until six (6) months after the expiration of this Contract. The Contractor will be liable for payment within thirty (30) days written notice of any liquidated damages or other offset

authorized by this Contract not deducted from any payment made by County to Contractor.

5.5.13 Fiscal Close-Out Report

Contractor must provide a Final Fiscal Close-Out Report, to be submitted in the form and manner designated by the County Contract Administrator, with a deadline to be announced for the CSBG Program, including a report of expenses and accruals through the last day of the calendar year.

5.5.14 Unspent Funds

5.5.14.1 At the end of each Calendar Year (CY) and at the end of the contract term, any excess funds and interest the Contractor has accumulated for the provision of CSBG services are to be treated as Unspent Funds.

5.5.14.2 At the County's sole discretion, these Unspent Funds may be retained by the Contractor to fund enhanced program related services but not the services already being provided by the Contractor. The use of the Unspent Funds must be reasonable and allowable.

5.5.14.3 Contractor will be responsible for tracking all Contract payments and expenditures for the program, including submission of the following:

1. An Expenditure Report on Contract revenues versus expenditures for each CY must be submitted to DPSS CAM on Jan 31st following the end of each CY and no later than one (1) month after the end of the contract term. Any revisions to the Expenditure Report must be submitted to CAM no later than ten (10) calendar days after submission of the original Report. The purpose of the Expenditure Report is to identify the amount of Unspent Funds and its earned interest. The Expenditure Report will be reviewed by the County.
2. The County reserves the right to change the Expenditure Report reporting periods.

5.5.14.4 A Disposition Plan on how the Unspent Funds and its earned interest will be reinvested must be submitted by the Contractor to the County with the Contractor's Expenditure Report.

1. Unspent Funds must be used to enhance the already approved programs services and must be spent on items above and beyond those items identified in the Contract and the Contract Budget.

The Disposition Plan must include a budget in accordance with the principles included in Office of Management and Budget (OMB) Super Circular

https://www.whitehouse.gov/omb/information-for-agencies/circulars/.

The Disposition Plan will be reviewed by the County and is subject to approval at the County's sole discretion. Unspent Funds must be used within the CY that the Disposition Plan is approved or within a time period determined by the County.

2. In addition, the Disposition Plan must include a detailed description of the services to be provided, the duration of those services, measurable outcomes, monitoring plan, all reporting and record keeping activities and a budget.
3. If the County does not approve the Contractor's Disposition Plan, the County will request the Unspent Funds and its earned interest be returned to the County within thirty (30) days after the County's disapproval of the Disposition Plan. The Contractor must comply with the County's request.
4. The County has the right to evaluate the effectiveness of services provided under the Disposition Plan. If the County finds the services are not effective, the services under the Disposition Plan may be terminated at the County's sole discretion and the Contractor must return the remaining Unspent Funds and its earned interest to the County.
5. The Contractor must submit a Final Disposition Report to the County within thirty (30) days after the scheduled completion date of an approved Disposition Plan. The Final Disposition Report must reflect the final status on the completion of all tasks included in the Disposition Plan, as well as all of the final outcomes of said tasks and a final statement on expenditures. Any Unspent Funds remaining after the completion of the approved Disposition Plan must be returned to the County with the Final Disposition Plan.

5.5.14.5 All uses of funds paid to and expended by Contractor, including Unspent Funds, and other financial transactions related to Contractor's provision of services

under this Contract are subject to review and/or audit by DPSS, County's Auditor-Controller or its designee.

5.5.14.6 Notwithstanding any other provision of this Contract, in addition to all other rights to monitor, Contractor and the County agree that it is the intent of the parties that the County will have the right to audit any and all use of funds paid to and expended by Contractor, including Unspent Funds and its earned interest, in order to ensure that all funds are accounted for by the County.

5.5.14.7 Contractor agrees to be bound by applicable federal, State and County disallowed cost principles and regulations, and to repay to County any amount, with its earned interest, which is found to violate the terms of this Contract or applicable provisions.

5.5.15 Funding/Budget Modification

5.5.15.1 Changes to the total funding as set forth in each Service Requisition may be made only by amendment to the Service Requisition signed by County and Contractor.

5.5.15.2 With regard to the movement of funds within an approved budget (i.e. from one line item to another), such movements in total may not exceed twenty-five percent (25%) of the Contract amount. Such modifications must be in writing and mutually agreed upon by the DPSS Director, or designee, and Contractor and such modification must be in the best interest of the County.

5.5.15.3 Contractor requests for modifications, either budgetary or programmatic, will not be accepted during the first two (2) months of the Service Requisition period, nor during the last quarter of the Service Requisition period (except where a written waiver is requested by the Contractor and accepted by the County or pursuant to Sub-paragraph 5.5.15.4). Furthermore, such requests will not be submitted to the County more than once in each quarter except where a written waiver has been received and accepted by the County.

5.5.15.4 Due to the natural discrepancies that may occur between budget projections and actual expenditures, the Contractor will be allowed to deviate no more than ten percent (10%) of the budgeted amount per line item without County's prior approval. Such budget

corrections among line-items will be allowed only upon reaching the final month of the Service Requisition term.

5.5.16 Reallocation of Funds

Contractor must maintain performance levels at percentage to be determined throughout the term of the Service Requisition. County will assess Contractor's performance level in the seventh month from the start date or any other month as determined by the County. If Contractor falls below indicated percentage of the year-to-date performance goals, by the following month or any other month as determined by the County, Contractor funds may be reduced and reallocated to other contractors who are meeting their performance goals. If Contractor meets and/or exceeds the indicated percentage of the performance goals, then Contractor may qualify for a funding increase. The County, at its sole discretion, may reduce the Contractor's total maximum Service Requisition amount for the following contract year to reflect the Contractor's level of service more accurately.

5.5.17 **Intentionally Omit**

5.6 Default Method of Payment: Direct Deposit or Electronic Funds Transfer

5.6.1 The County, at its sole discretion, has determined that the most efficient and secure default form of payment for goods and/or services provided under an agreement/contract with the County will be Electronic Funds Transfer (EFT) or direct deposit, unless an alternative method of payment is deemed appropriate by the Auditor-Controller (A-C).

5.6.2 The Contractor must submit a direct deposit authorization request via the website https://directdeposit.lacounty.gov with banking and vendor information, and any other information that the A-C determines is reasonably necessary to process the payment and comply with all accounting, record keeping, and tax reporting requirements.

5.6.3 Any provision of law, grant, or funding agreement requiring a specific form or method of payment other than EFT or direct deposit will supersede this requirement with respect to those payments.

5.6.4 At any time during the duration of the agreement/contract, a Contractor may submit a written request for an exemption to this requirement. Such request must be based on specific legal, business or operational needs and explain why the payment method designated by the A-C is not feasible and an alternative is necessary. The A-C, in consultation with the contracting

department(s), will decide whether to approve exemption requests.

5.7 Fiscal Accountability

5.7.1 Fiscal Policies/Procedures

The Contractor will be required to adhere to strict fiscal and accounting standards and must comply with Title 2 of the Code of Federal Regulations Part 200 (2 CFR 200 et seq.) and related OMB Guidance.

5.7.2 Compliance with Auditor Controller Contract Accounting and Administration Handbook

The County recommends the use of the accrual basis for recording financial transactions. The Auditor-Controller Handbook establishes the minimum required accounting, financial reporting, and internal control standards for entities (Contractors) which contract with the County. Contractor will refer to the Auditor-Controller Handbook at:

https://auditor.lacounty.gov/wp-content/uploads/2022/05/A-C-Handbook-Revised-June-2021.pdf

5.7.3 Cost Allocation

5.7.3.1 Allocation of Cost Pools

For Contractors that provide services in addition to the services provided pursuant to Service Requisition(s) under the Master Agreement, the Contractor must allocate expenditures that benefit programs, or funding sources on an equitable basis.

In accordance with the applicable OMB Uniform Guidance, agencies must define their allocable costs as either direct or indirect costs and allocate each cost using the basis most appropriate and feasible.

The Contractor must maintain documentation related to the allocation of expenses (e.g., timecards, time summaries, square footage measurements, number of employees, etc.)

Under no circumstances will allocated costs be charged to an extent greater than one hundred (100%) percent of actual costs or the same cost be charged both directly and indirectly.

5.7.3.2 Cost Allocation Plan

If the Contractor has a negotiated indirect cost rate approved by a federal agency, it must submit a copy of

the approval letter when requested by County or immediately following the execution of this Contract.

Contractor must submit an annual Agency-wide Cost Allocation Plan when requested by the County. The Cost Allocation Plan must be prepared in accordance with County instructions and the applicable sections of the OMB Uniform Guidance and include the following information:

1. Contractor General Accounting Policies:
    - Basis of accounting (cash or accrual),
    - Fiscal Year,
    - Method for allocating indirect costs (simplified, direct, multiple, negotiated rate, de minimis rate), and
    - Indirect cost rate allocation base.
2. Identify the Contractor's direct and indirect costs (by each category) and describe the cost allocation methodology for each category.
3. Signature of Contractor management certifying the accuracy of plan.

For more clarification see Auditor-Controller Handbook, at the link provided in Paragraph 5.7.2.

5.7.4 The Contractor must establish and maintain a financial management system, which provides for adequate control of Program funds and other assets; ensures adequacy of financial data; and provides operational efficiency and adequate internal controls. Failure to comply with this Paragraph 5.6.4 may, in addition to other remedies available to the County, result in withholding of payment to the Contractor, suspension, or termination of the contract in accordance with its terms.

5.7.5 Funds paid pursuant to a Service Requisition must be used exclusively for services funded under the Service Requisition and must not be commingled with any other monies of the Contractor unless a written waiver is obtained from the County.

6.0 ADMINISTRATION OF MASTER AGREEMENT – COUNTY

6.1 County's Administration

A listing of all County Administration referenced in the following Subsections are designated in Exhibit B (County's Administration). The County will notify the Contractor in writing of any change in the names or addresses shown.

6.2 County Contract Director

County will designate one person who will have the authority to act as the County Contract Director on all matters pertaining to this Master Agreement. Responsibilities of the County Contract Director or alternate include:

6.2.1 Ensuring that the objectives of this Master Agreement are met; and

6.2.2 Providing direction to Contractor on contractual or administrative matters relating to this Master Agreement that cannot be resolved by the Supervising County Contract Administrator, described in Subsection 6.3, below.

The County Contract Director is not authorized to make any changes in any of the terms and conditions of this Master Agreement and is not authorized to further obligate the County in any respect whatsoever, except through formally prepared amendments and change notices, Subsection 8.1.

6.3 Supervising County Contract Administrator

County will designate one person who will have the authority to act as the Supervising County Contract Administrator on all matters pertaining to this Master Agreement. Responsibilities of the Supervising County Contract Administrator or alternate include:

6.3.1 Overseeing the overall management and administration of the Master Agreement; and

6.3.2 Providing direction to Contractor on contractual or administrative matters relating to this Master Agreement that cannot be resolved by the County Contract Administrator, described in Subsection 6.4 below.

The Supervising County Contract Administrator is not authorized to make any changes in any of the terms and conditions of this Master Agreement and is not authorized to further obligate the County in any respect whatsoever.

6.4 County Contract Administrator

County will designate one person who will have the authority to act as the County Contract Administrator on administrative matters pertaining to this Master Agreement. Responsibilities of the County Contract Administrator or alternate include:

6.4.1 Overseeing the day-to-day administration of the Master Agreement;

6.4.2 Ensuring that the Master Agreement objectives are met;

6.4.3 Providing direction to Contractor in the areas relating to the Master Agreement, Service Requisition, invoicing, and administrative procedural requirements.

6.4.4 Monitoring, evaluating and reporting Contractor performance and progress on the Service Requisition;

6.4.5 Coordinating with Contractor's Contract Manager, on a regular basis, regarding the performance of Contractor's personnel on each particular project;

6.4.6 Evaluating any and all Master Agreement and Service Requisition related tasks, deliverable goods, services, data, or other work provided by or on behalf of Contractor; and

6.4.7 Meeting with the Contractor's Contract Manager on a regular basis.

The County Contract Administrator is not authorized to make any changes in the terms and conditions of this Master Agreement, and is not authorized to further obligate the County in any respect whatsoever.

6.5 County Contract Program Manager

County will designate one person who will have the authority to act as the County Contract Program Manager on all policy, program and operational matters of the Master Agreement and Service Requisition. Responsibilities of the County Contract Program Manager or alternate include:

6.5.1 Providing direction to Contractor in the areas of County policy and program requirements;

6.5.2 Ensuring that the outcomes of the Master Agreement and Service Requisition are met; and

6.5.3 Evaluating any and all program related tasks, deliverables, goods, services, data, or other work provided by or on behalf of the Contractor.

The County Contract Program Manager is not authorized to make any changes in any of the terms and conditions of this Master Agreement and is not authorized to further obligate the County in any respect whatsoever.

6.6 County Contract Program Monitor (CPM)

County will designate one staff who will have the authority to act as the County's CPM. The responsibilities of the County's CPM or alternate include:

6.6.1 Providing direction to Contractor in the areas of County policy and program requirements;

6.6.2 Providing assistance to the County Contract Administrator in overseeing day-to-day administration of the Master Agreement and Service Requisition;

6.6.3 Ensuring all outcomes of Master Agreement and Service Requisition are met; and

6.6.4 Monitoring and evaluating any and all tasks, deliverables, goods, services provided by Contractor and Contractor's compliance with the Master Agreement and/or Service Requisition terms.

The County's CPM is not authorized to make any changes in any of the terms and conditions of this Contract and is not authorized to further obligate the County in any respect whatsoever.

7.0 ADMINISTRATION OF MASTER AGREEMENT - CONTRACTOR

7.1 Contractor's Contract Manager

7.1.1 Contractor's Contract Manager is designated in Exhibit C (Contractor's Administration). The Contractor must notify the County in writing of any change in the name or address of the Contractor's Contract Manager.

7.1.2 Contractor's Contract Manager will be responsible for Contractor's day-to-day activities as related to this Master Agreement and will coordinate with County Contract Administrator and/or County CPM (upon County Contract Administrator approval) on a regular basis with respect to all active Service Requisitions.

7.1.3 Contractor's Contract Manager, or alternate, designated in writing to act on the Contractor's behalf, must be available to respond to the County's verbal inquiries within one (1) business day, excluding weekends and holidays.

7.2 Contractor's Authorized Official(s)

7.2.1 Contractor's Authorized Official(s) are designated in Exhibit C (Contractor's Administration). Contractor must promptly notify County in writing of any change in the name(s) or address(es) of Contractor's Authorized Official(s).

7.2.2 Contractor represents and warrants that all requirements of Contractor have been fulfilled to provide actual authority to such officials to execute documents under this Master Agreement on behalf of Contractor.

7.2.3 Contractor must provide a list of authorized signers and a list of the agency's Board of Directors on an annual basis, or at any time there is a change.

7.3 Approval of Contractor's Staff

County has the absolute right to approve or disapprove all of Contractor's staff performing work hereunder and any proposed changes in Contractor's staff, including, but not limited to, Contractor's Contract Manager. Contractor must provide County with a résumé of each proposed substitute and an opportunity to interview such person prior to any staff substitution.

7.4 Contractor's Staff Identification

Contractor will provide, at Contractor's expense, all staff providing services under this Master Agreement with a photo identification badge.

7.5 Background and Security Investigations

7.5.1 Each of Contractor's staff performing services under this Master Agreement who is in a designated sensitive position, as determined by County in County's sole discretion, must undergo and pass a background investigation to the satisfaction of County as a condition of beginning and continuing to perform services under this Master Agreement. Such background investigation must be obtained through fingerprints submitted to the California Department of Justice to include State, local, and federal-level review, which may include, but will not be limited to, criminal conviction information. The fees associated with the background investigation will be at the expense of the Contractor, regardless if the member of Contractor's staff passes or fails the background investigation.

7.5.2 If a member of Contractor's staff does not pass the background investigation, County may request that the member of Contractor's staff be immediately removed from performing services under the Master Agreement at any time during the term of the Master Agreement. County will not provide to Contractor or to Contractor's staff any information obtained through the County's background investigation.

7.5.3 County, in its sole discretion, may immediately deny or terminate facility access to any member of Contractor's staff that does not pass such investigation to the satisfaction of the County or whose background or conduct is incompatible with County facility access.

7.5.4 Disqualification of any member of Contractor's staff pursuant to this Subsection 7.5 will not relieve Contractor of its obligation to complete all work in accordance with the terms and conditions of this Master Agreement.

7.6 Confidentiality

7.6.1 Contractor must maintain the confidentiality of all records and information in accordance with all applicable federal, State and local laws, rules, regulations, ordinances, directives, guidelines, policies and procedures relating to confidentiality, including, without limitation, County policies concerning information technology security and the protection of confidential records and information.

7.6.2 Contractor must indemnify, defend, and hold harmless County, its officers, employees, and agents, from and against any and all

claims, demands, damages, liabilities, losses, costs and expenses, including, without limitation, defense costs and legal, accounting and other expert, consulting, or professional fees, arising from, connected with, or related to any failure by Contractor, its officers, employees, agents, or Subcontractors, to comply with this Subsection 7.6, as determined by County in its sole judgment. Any legal defense pursuant to Contractor's indemnification obligations under this Subsection 7.6 will be conducted by Contractor and performed by counsel selected by Contractor and approved by County. Notwithstanding the preceding sentence, County will have the right to participate in any such defense at its sole cost and expense, except that in the event Contractor fails to provide County with a full and adequate defense, as determined by County in its sole judgment, County will be entitled to retain its own counsel, including, without limitation, County Counsel, and reimbursement from Contractor for all such costs and expenses incurred by County in doing so. Contractor will not have the right to enter into any settlement, agree to any injunction, or make any admission, in each case, on behalf of County without County's prior written approval.

7.6.3 Contractor must inform all of its officers, employees, agents and Subcontractors providing services hereunder of the confidentiality provisions of this Master Agreement.

7.6.4 Contractor must sign and adhere to the provisions of the Exhibit E-1 (Contractor Acknowledgement and Confidentiality Agreement).

7.6.5 Contractor will cause each employee performing services covered by this Master Agreement to sign and adhere to the provisions of Exhibit E-2 (Contractor Employee Acknowledgment and Confidentiality Agreement).

7.6.6 Contractor will cause each non-employee performing services covered by this Master Agreement to sign and adhere to the provisions of Exhibit E-3 (Contractor Non-Employee Acknowledgment and Confidentiality Agreement).

7.6.7 By State law (See Welfare and Institution Code, Sections 10850 et seq. and 17006), including without limitation all of the case records and information pertaining to individuals receiving aid are confidential and no information related to any individual case or cases is to be in any way relayed to anyone except those employees of the Los Angeles County DPSS so designated, without written authorization from DPSS.

8.0 STANDARD TERMS AND CONDITIONS

8.1 Amendments and Change Notices

8.1.1 The County reserves the right to initiate Change Notices that do not materially affect the scope of work, term, Contract Sum, payment terms or any other term or condition under this Master Agreement. All such changes will be accomplished with a Change Notice signed by the Contractor and by the County Contract Director.

8.1.2 For any change which materially affects the scope of work, term of the Master Agreement, Contract Sum, payment terms, or any other term or condition under the Master Agreement, an Amendment must be prepared and executed by the Contractor and by the DPSS Director or designee.

8.1.3 The County's Board or Chief Executive Officer or designee may require the addition and/or change of certain terms and conditions in the Master Agreement during the term of this Master Agreement. The County reserves the right to add and/or change such provisions as required by the County's Board or Chief Executive Officer. To implement such orders, an Amendment to the Master Agreement must be prepared and executed by the Contractor and by the DPSS Director or designee.

8.1.4 The DPSS Director, or their designee, may, at their sole discretion, authorize extensions of time as defined in Section 4.0 (Term of Master Agreement). The Contractor agrees that such extensions of time will not change any other term or condition of this Master Agreement during the period of such extensions. To implement an extension of time, an Amendment to the Master Agreement must be prepared and executed by the Contractor and by the DPSS Director or designee.

8.2 Assignment and Delegation/Mergers or Acquisitions

8.2.1 The Contractor must notify the County of any pending acquisitions/mergers of its company unless otherwise legally prohibited from doing so. If the Contractor is restricted from legally notifying the County of pending acquisitions/mergers, then it should notify the County of the actual acquisitions/mergers as soon as the law allows and provide to the County the legal framework that restricted it from notifying the County prior to the actual acquisitions/mergers.

8.2.2 The Contractor must not assign, exchange, transfer, or delegate its rights or duties under this Master Agreement, whether in whole or in part, without the prior written consent of County, in its discretion, and any attempted assignment, delegation, or

otherwise transfer of its rights or duties, without such consent will be null and void. For purposes of this Paragraph, County consent will require a written amendment to the Master Agreement, which is formally approved and executed by the parties. Any payments by the County to any approved delegate or assignee on any claim under this Master Agreement will be deductible, at County's sole discretion, against the claims, which the Contractor may have against the County.

8.2.3 Any assumption, assignment, delegation, or takeover of any of the Contractor's duties, responsibilities, obligations, or performance of same by any person or entity other than the Contractor, whether through assignment, subcontract, delegation, merger, buyout, or any other mechanism, with or without consideration for any reason whatsoever without County's express prior written approval, will be a material breach of the Master Agreement which may result in the termination of this Master Agreement. In the event of such termination, County will be entitled to pursue the same remedies against Contractor as it could pursue in the event of default by Contractor.

8.3 Authorization Warranty

The Contractor represents and warrants that the person executing this Master Agreement for the Contractor is an authorized agent who has actual authority to bind the Contractor to each and every term, condition, and obligation of this Master Agreement and that all requirements of the Contractor have been fulfilled to provide such actual authority.

8.4 Complaints

The Contractor must develop, maintain, and operate procedures for receiving, investigating and responding to complaints.

8.4.1 Within five (5) business days after the Master Agreement effective date, the Contractor must provide the County with the Contractor's policy for receiving, investigating and responding to user complaints.

8.4.2 The County will review the Contractor's policy and provide the Contractor with approval of said plan or with requested changes.

8.4.3 If the County requests changes in the Contractor's policy, the Contractor must make such changes and resubmit the plan within five (5) business days for County approval.

8.4.4 If, at any time, the Contractor wishes to change the Contractor's policy, the Contractor must submit proposed changes to the County for approval before implementation.

8.4.5 The Contractor must preliminarily investigate all complaints and notify the County Contract Director of the status of the investigation within five (5) business days of receiving the complaint.

8.4.6 When complaints cannot be resolved informally, a system of follow-through will be instituted which adheres to formal plans for specific actions and strict time deadlines.

8.4.7 Copies of all written responses must be sent to the County Contract Director within three (3) business days of mailing to the complainant.

8.5 Compliance with Applicable Laws

8.5.1 In the performance of this Master Agreement, Contractor must comply with all applicable federal, State and local laws, rules, regulations, ordinances, directives, guidelines, policies and procedures, and all provisions required thereby to be included in this Master Agreement are hereby incorporated herein by reference.

8.5.2 Contractor must indemnify, defend, and hold harmless County, its officers, employees, and agents, from and against any and all claims, demands, damages, liabilities, losses, costs, and expenses, including, without limitation, defense costs and legal, accounting and other expert, consulting or professional fees, arising from, connected with, or related to any failure by Contractor, its officers, employees, agents, or Subcontractors, to comply with any such laws, rules, regulations, ordinances, directives, guidelines, policies, or procedures, as determined by County in its sole judgment. Any legal defense pursuant to Contractor's indemnification obligations under this Subsection 8.5 will be conducted by Contractor and performed by counsel selected by Contractor and approved by County. Notwithstanding the preceding sentence, County will have the right to participate in any such defense at its sole cost and expense, except that in the event Contractor fails to provide County with a full and adequate defense, as determined by County in its sole judgment, County will be entitled to retain its own counsel, including, without limitation, County Counsel, and reimbursement from Contractor for all such costs and expenses incurred by County in doing so. Contractor will not have the right to enter into any settlement, agree to any injunction or other equitable relief, or make any admission, in each case, on behalf of County without County's prior written approval.

8.6 Compliance with Civil Rights Laws

The Contractor must abide by the provisions of Title VI and Title VII of the Federal Civil Rights Act of 1964, as amended; Section 504 of the

Rehabilitation Act of 1973, as amended; the Age Discrimination Act of 1975; the Food Stamp Act of 1977, as amended; the ADA of 1990, as amended; Welfare and Institutions Code (W&IC) Section 10000; California Department of Social Services (CDSS) Manual of Policies and Procedures, Division 21; and other applicable federal and State laws to ensure that employment practices and the delivery of social service programs are nondiscriminatory. Under this requirement, Contractor will not discriminate on the basis of race, color, ancestry, national origin (including language), ethnic group identification, political affiliation, citizenship, immigration status, religion, marital status, domestic partnership, age, physical or mental disability, medical condition, sex, gender, gender identity or expression, sexual orientation, and genetic information, or retaliate against an individual engaging in a protected activity, such as filing a complaint, complaint, testifying or participating in any manner in any investigation, proceeding, or hearing, and in compliance with all anti-discrimination laws of the United States of America and the State of California. Contractor must sign and adhere with the terms as set forth in Exhibit I, Contractor's EEO Certification, and Exhibit J, Non-Discrimination In-Services Certification.

In addition, Contractor must abide by the provisions contained in the current Civil Rights Training Handbook, which was developed in compliance with the Civil Rights Resolution Agreement between Los Angeles County and the Federal Office for Civil Rights, Department of Health and Human Services. The Civil Rights Training Handbook incorporates the Civil Rights requirements of the Resolution Agreement along with all other mandated federal and State requirements that must be adhered to by DPSS and its Contractors and Subcontractors. Civil Rights requirements include, but are not limited to the following:

8.6.1 Ensure that public contact staff attend DPSS provided mandatory Civil Rights Training every two years and ADA Title II training every year, retaining verification on file and providing to DPSS upon request. Contractor must contact the County Contract Administrator to coordinate said trainings.

8.6.2 Effectively identify customers' designated preferred language.

8.6.3 Ensure that all written documents provided to customers are provided in their preferred language.

8.6.4 Provide interpreters in the customers' preferred language to ensure meaningful access to services without undue delay.

8.6.5 Maintain records that include any Civil Rights-related correspondence to participants, such as the Interpreter Services Statement and Confidentiality Agreement (CR 6181), which is used to document language services requirements when customers use their own interpreter; inform customers about risks when they use their own interpreter; document customers own interpreter confidentiality agreement; and document in the case

records whether language services and ADA accommodations were provided.

8.6.6 Ensure that the PUB 13, Your Rights Under California Benefits Programs and PA 2457, Civil Rights Information Notice is explained and reviewed with all customers and made available in all waiting areas in all DPSS threshold languages.

8.6.7 Collect data necessary to monitor compliance with Civil Rights Requirements.

8.6.8 Ensure that all complaints of discriminatory treatment, including alleged ADA violations, are listed on an internal complaint log.

8.6.9 Follow steps outlined in the Civil Rights Complaint Flowchart Process for Contractors for processing of discrimination complaints from DPSS customers.

A copy of the Civil Rights Training Handbook may be obtained by contacting the County Contract Administrator.

8.7 Compliance with County's Jury Service Program

8.7.1 Jury Service Program**:** This Master Agreement is subject to the provisions of the County's ordinance entitled Contractor Employee Jury Service ("Jury Service Program") as codified in Sections 2.203.010 through 2.203.090 of the Los Angeles County Code, a copy of which is attached as Exhibit L and incorporated by reference into and made part of this Master Agreement.

8.7.2 Written Employee Jury Service Policy

1. Unless Contractor has demonstrated to the County's satisfaction either that Contractor is not a "Contractor" as defined under the Jury Service Program (Section 2.203.020 of the County Code) or that Contractor qualifies for an exception to the Jury Service Program (Section 2.203.070 of the County Code), Contractor must have and adhere to a written policy that provides that its Employees will receive from the Contractor, on an annual basis, no less than five days of regular pay for actual jury service. The policy may provide that Employees deposit any fees received for such jury service with the Contractor or that the Contractor deduct from the Employee's regular pay the fees received for jury service.

2. For purposes of this Paragraph, "Contractor" means a person, partnership, corporation or other entity which has a Master Agreement with the County or a subcontract with a County Contractor and has received or will receive an aggregate sum of $50,000 or more in any 12-month period under one or more County Master Agreements or subcontracts. "Employee" means any California resident who is a full-time employee of

Contractor. “Full-time” means 40 hours or more worked per week, or a lesser number of hours if: 1) the lesser number is a recognized industry standard as determined by the County, or 2) Contractor has a long-standing practice that defines the lesser number of hours as full-time. Full-time employees providing short-term, temporary services of 90 days or less within a 12-month period are not considered full-time for purposes of the Jury Service Program. If Contractor uses any Subcontractor to perform services for the County under the Master Agreement, the Subcontractor will also be subject to the provisions of this paragraph. The provisions of this paragraph will be inserted into any such subcontract agreement and a copy of the Jury Service Program must be attached to the agreement.

3. If Contractor is not required to comply with the Jury Service Program when the Master Agreement commences, Contractor will have a continuing obligation to review the applicability of its “exception status” from the Jury Service Program, and Contractor must immediately notify County if Contractor at any time either comes within the Jury Service Program’s definition of “Contractor” or if Contractor no longer qualifies for an exception to the Jury Service Program. In either event, Contractor must immediately implement a written policy consistent with the Jury Service Program. The County may also require, at any time during the Master Agreement and at its sole discretion, that Contractor demonstrate to the County’s satisfaction that Contractor either continues to remain outside of the Jury Service Program’s definition of “Contractor” and/or that Contractor continues to qualify for an exception to the Program.

4. Contractor’s violation of this Paragraph of the Master Agreement may constitute a material breach of the Master Agreement. In the event of such material breach, County may, in its sole discretion, terminate the Master Agreement and/or bar Contractor from the award of future County Master Agreements for a period of time consistent with the seriousness of the breach.

8.8 Conflict of Interest

8.8.1 No County employee whose position with the County enables such employee to influence the award of this Master Agreement or any competing Master Agreement, and no spouse or economic dependent of such employee, will be employed in any capacity by the Contractor or have any other direct or indirect financial interest in this Master Agreement. No officer or employee of the Contractor who may financially benefit from the performance of work

hereunder will in any way participate in the County's approval, or ongoing evaluation, of such work, or in any way attempt to unlawfully influence the County's approval or ongoing evaluation of such work.

8.8.2 The Contractor must comply with all conflict of interest laws, ordinances, and regulations now in effect or hereafter to be enacted during the term of this Master Agreement. The Contractor warrants that it is not now aware of any facts that create a conflict of interest. If the Contractor hereafter becomes aware of any facts that might reasonably be expected to create a conflict of interest, it must immediately make full written disclosure of such facts to the County. Full written disclosure must include, but is not limited to, identification of all persons implicated and a complete description of all relevant circumstances. Failure to comply with the provisions of this Subsection 8.8 will be a material breach of this Master Agreement.

8.9 Consideration of Hiring County Employees Targeted for Layoffs or are on a County Re-employment List

Should the Contractor require additional or replacement personnel after the effective date of this Master Agreement to perform the services set forth herein, the Contractor must give first consideration for such employment openings to qualified, permanent County employees who are targeted for layoff or qualified, former County employees who are on a re-employment list during the life of this Master Agreement.

8.10 Consideration of Hiring GAIN/START Participants

8.10.1 Should the Contractor require additional or replacement personnel after the effective date of this Master Agreement, the Contractor will give consideration for any such employment openings to participants in the County's Department of Public Social Services Greater Avenues for Independence (GAIN) Program or Skills and Training to Achieve Readiness for Tomorrow (START) Program who meet the Contractor's minimum qualifications for the open position. For this purpose, consideration will mean that the Contractor will interview qualified candidates. The County will refer GAIN/START participants by job category to the Contractor. Contractors must report all job openings with job requirements to: gainstart@dpss.lacounty.gov and bservices@opportunity.lacounty.gov and DPSS will refer qualified GAIN/START job candidates.

8.10.2 In the event that both laid-off County employees and GAIN/START participants are available for hiring, County employees must be given first priority.

8.11 Contractor Responsibility and Debarment

8.11.1 Responsible Contractor

A responsible Contractor is a Contractor who has demonstrated the attribute of trustworthiness, as well as quality, fitness, capacity and experience to satisfactorily perform the Master Agreement. It is the County's policy to conduct business only with responsible Contractors.

8.11.2 Chapter 2.202 of the County Code

The Contractor is hereby notified that, in accordance with Chapter 2.202 of the County Code, if the County acquires information concerning the performance of the Contractor on this or other Master Agreements which indicates that the Contractor is not responsible, the County may, in addition to other remedies provided in this Master Agreement, debar the Contractor from bidding or proposing on, or being awarded, and/or performing work on County contracts for a specified period of time, which generally will not exceed five years but may exceed five years or be permanent if warranted by the circumstances, and terminate any or all existing Contracts the Contractor may have with the County.

8.11.3 Non-responsible Contractor

The County may debar a Contractor if the Board of Supervisors finds, in its discretion, that the Contractor has done any of the following: (1) violated a term of a Master Agreement with the County or a nonprofit corporation created by the County, (2) committed an act or omission which negatively reflects on the Contractor's quality, fitness or capacity to perform a Master Agreement with the County, any other public entity, or a nonprofit corporation created by the County, or engaged in a pattern or practice which negatively reflects on same, (3) committed an act or offense which indicates a lack of business integrity or business honesty, or (4) made or submitted a false claim against the County or any other public entity.

8.11.4 Contractor Hearing Board

- If there is evidence that the Contractor may be subject to debarment, the Department will notify the Contractor in writing of the evidence which is the basis for the proposed debarment and will advise the Contractor of the scheduled date for a debarment hearing before the Contractor Hearing Board.
- The Contractor Hearing Board will conduct a hearing where evidence on the proposed debarment is presented. The Contractor and/or the Contractor's representative will be given an opportunity to submit evidence at that hearing. After the

hearing, the Contractor Hearing Board will prepare a tentative proposed decision, which will contain a recommendation regarding whether the Contractor should be debarred, and, if so, the appropriate length of time of the debarment. The Contractor and the Department will be provided an opportunity to object to the tentative proposed decision prior to its presentation to the Board of Supervisors.

- After consideration of any objections, or if no objections are submitted, a record of the hearing, the proposed decision, and any other recommendation of the Contractor Hearing Board will be presented to the Board of Supervisors. The Board of Supervisors will have the right to modify, deny, or adopt the proposed decision and recommendation of the Contractor Hearing Board.
- If a Contractor has been debarred for a period longer than five (5) years, that Contractor may after the debarment has been in effect for at least five (5) years, submit a written request for review of the debarment determination to reduce the period of debarment or terminate the debarment. The County may, in its discretion, reduce the period of debarment or terminate the debarment if it finds that the Contractor has adequately demonstrated one or more of the following: (1) elimination of the grounds for which the debarment was imposed; (2) a bona fide change in ownership or management; (3) material evidence discovered after debarment was imposed; or (4) any other reason that is in the best interests of the County.
- The Contractor Hearing Board will consider a request for review of a debarment determination only where (1) the Contractor has been debarred for a period longer than five (5) years; (2) the debarment has been in effect for at least five (5) years; and (3) the request is in writing, states one or more of the grounds for reduction of the debarment period or termination of the debarment, and includes supporting documentation. Upon receiving an appropriate request, the Contractor Hearing Board will provide notice of the hearing on the request. At the hearing, the Contractor Hearing Board will conduct a hearing where evidence on the proposed reduction of debarment period or termination of debarment is presented. This hearing will be conducted and the request for review decided by the Contractor Hearing Board pursuant to the same procedures as for a debarment hearing.
- The Contractor Hearing Board's proposed decision will contain a recommendation on the request to reduce the period of debarment or terminate the debarment. The Contractor Hearing Board will present its proposed decision

and recommendation to the Board of Supervisors. The Board of Supervisors will have the right to modify, deny, or adopt the proposed decision and recommendation of the Contractor Hearing Board.

8.11.5 Subcontractors of Contractor

These terms will also apply to Subcontractors of County Contractors.

8.12 Contractor's Acknowledgement of County's Commitment to Safely Surrendered Baby Law

The Contractor acknowledges that the County places a high priority on the implementation of the Safely Surrendered Baby Law. The Contractor understands that it is the County's policy to encourage all County Contractors to voluntarily post the County's "Safely Surrendered Baby Law" poster, in Exhibit D, in a prominent position at the Contractor's place of business. The Contractor will also encourage its Subcontractors, if any, to post this poster in a prominent position in the Subcontractor's place of business. Information and posters for printing are available at:

https://lacounty.gov/residents/family-services/child-safety/safe-surrender/

8.13 Contractor's Warranty of Adherence to County's Child Support Compliance Program

8.13.1 The Contractor acknowledges that the County has established a goal of ensuring that all individuals who benefit financially from the County through Service Requisition or Master Agreement are in compliance with their court-ordered child, family and spousal support obligations in order to mitigate the economic burden otherwise imposed upon the County and its taxpayers.

8.13.2 As required by the County's Child Support Compliance Program (County Code Chapter 2.200) and without limiting the Contractor's duty under this Master Agreement to comply with all applicable provisions of law, the Contractor warrants that it is now in compliance and will during the term of this Master Agreement maintain compliance with employment and wage reporting requirements as required by the Federal Social Security Act (42 USC Section 653a) and California Unemployment Insurance Code Section 1088.5, and will implement all lawfully served Wage and Earnings Withholding Orders or Child Support Services Department Notices of Wage and Earnings Assignment for Child, Family or Spousal Support, pursuant to Code of Civil Procedure Section 706.031 and Family Code Section 5246(b).

8.14 County's Quality Assurance Plan

The County or its agent(s) will monitor the Contractor's performance under this Master Agreement on not less than an annual basis. Such monitoring will

include assessing the Contractor's compliance with all Master Agreement terms and conditions and performance standards. Contractor deficiencies which the County determines are significant or continuing and that may place performance of the Master Agreement in jeopardy if not corrected will be reported to the Board of Supervisors and listed in the appropriate contractor performance database. The report to the Board will include improvement/ corrective action measures taken by the County and the Contractor. If improvement does not occur consistent with the corrective action measures, the County may terminate this Master Agreement or impose other penalties as specified in this Master Agreement.

8.15 Damage to County Facilities, Buildings or Grounds

8.15.1 The Contractor will repair, or cause to be repaired, at its own cost, any and all damage to County facilities, buildings, or grounds caused by Contractor or employees or agents of Contractor. Such repairs must be made immediately after Contractor has become aware of such damage, but in no event later than thirty (30) days after the occurrence.

8.15.2 If the Contractor fails to make timely repairs, County may make any necessary repairs. All costs incurred by County, as determined by County, for such repairs must be repaid by Contractor by cash payment upon demand.

8.16 Employment Eligibility Verification

8.16.1 The Contractor warrants that it fully complies with all federal and State statutes and regulations regarding the employment of aliens and others and that all its employees performing work under this Master Agreement meet the citizenship or alien status requirements set forth in federal and State statutes and regulations. The Contractor must obtain, from all employees performing work hereunder, all verification and other documentation of employment eligibility status required by federal and State statutes and regulations including, but not limited to, the Immigration Reform and Control Act of 1986, (P.L. 99-603), or as they currently exist and as they may be hereafter amended. The Contractor must retain all such documentation for all covered employees for the period prescribed by law.

8.16.2 The Contractor must indemnify, defend, and hold harmless, the County, its agents, officers, and employees from employer sanctions and any other liability which may be assessed against the Contractor or the County or both in connection with any alleged violation of any federal or State statutes or regulations pertaining to the eligibility for employment of any persons performing work under this Master Agreement.

8.17 Counterparts and Electronic Signatures and Representations

This Master Agreement may be executed in two or more counterparts, each of which will be deemed an original but all of which together will constitute one and the same Master Agreement. The facsimile, email or electronic signature of the Parties will be deemed to constitute original signatures, and facsimile or electronic copies hereof will be deemed to constitute duplicate originals.

The County and the Contractor hereby agree to regard electronic representations of original signatures of authorized officers of each party, when appearing in appropriate places on the Amendments and Change Notices prepared pursuant to Subsection 8.1 (Amendments and Change Notices) and received via communications facilities (facsimile, email or electronic signature), as legally sufficient evidence that such legally binding signatures have been affixed to Amendments and Change Notices to this Master Agreement and resulting Service Requisitions.

8.18 Fair Labor Standards

The Contractor must comply with all applicable provisions of the Federal Fair Labor Standards Act and must indemnify, defend, and hold harmless the County and its agents, officers, and employees from any and all liability, including, but not limited to, wages, overtime pay, liquidated damages, penalties, court costs, and attorneys' fees arising under any wage and hour law, including, but not limited to, the Federal Fair Labor Standards Act, for work performed by the Contractor’s employees for which the County may be found jointly or solely liable.

8.19 Force Majeure

8.19.1 Neither party will be liable for such party's failure to perform its obligations under and in accordance with this Master Agreement, if such failure arises out of fires, floods, epidemics, quarantine restrictions, other natural occurrences, strikes, lockouts (other than a lockout by such party or any of such party's Subcontractors), freight embargoes, or other similar events to those described above, but in every such case the failure to perform must be totally beyond the control and without any fault or negligence of such party (such events are referred to in this Paragraph as "force majeure events").

8.19.2 Notwithstanding the foregoing, a default by a Subcontractor of Contractor will not constitute a force majeure event, unless such default arises out of causes beyond the control of both Contractor and such Subcontractor, and without any fault or negligence of either of them. In such case, Contractor will not be liable for failure to perform, unless the goods or services to be furnished by the Subcontractor were obtainable from other sources in sufficient time to permit Contractor to meet the required performance

schedule. As used in this Paragraph, the term “Subcontractor” and “Subcontractors” mean Subcontractors at any tier.

8.19.3 In the event Contractor's failure to perform arises out of a force majeure event, Contractor agrees to use commercially reasonable best efforts to obtain goods or services from other sources, if applicable, and to otherwise mitigate the damages and reduce the delay caused by such force majeure event.

8.20 Governing Law, Jurisdiction, and Venue

This Master Agreement will be governed by, and construed in accordance with, the laws of the State of California. The Contractor agrees and consents to the exclusive jurisdiction of the courts of the State of California for all purposes regarding this Master Agreement and further agrees and consents that venue of any action brought hereunder will be exclusively in the County of Los Angeles.

8.21 Independent Contractor Status

8.21.1 This Master Agreement is by and between the County and the Contractor and is not intended, and must not be construed, to create the relationship of agent, servant, employee, partnership, joint venture, or association, as between the County and the Contractor. The employees and agents of one party must not be, or be construed to be, the employees or agents of the other party for any purpose whatsoever.

8.21.2 The Contractor will be solely liable and responsible for providing to, or on behalf of, all persons performing work pursuant to this Master Agreement all compensation and benefits. The County will have no liability or responsibility for the payment of any salaries, wages, unemployment benefits, disability benefits, federal, State, or local taxes, or other compensation, benefits, or taxes for any personnel provided by or on behalf of the Contractor.

8.21.3 The Contractor understands and agrees that all persons performing work pursuant to this Master Agreement are, for purposes of Workers' Compensation liability, solely employees of the Contractor and not employees of the County. The Contractor will be solely liable and responsible for furnishing any and all Workers' Compensation benefits to any person as a result of any injuries arising from or connected with any work performed by or on behalf of the Contractor pursuant to this Master Agreement.

8.21.4 The Contractor must adhere to the provisions stated in Subsection 7.6 (Confidentiality).

8.22 Indemnification

The Contractor must indemnify, defend and hold harmless the County, its Special Districts, elected and appointed officers, employees, agents and

volunteers (“County Indemnitees”) from and against any and all liability, including but not limited to demands, claims, actions, fees, costs and expenses (including attorney and expert witness fees), arising from and/or relating to this Master Agreement, except for such loss or damage arising from the sole negligence or willful misconduct of the County Indemnities.

8.23 General Provisions for all Insurance Coverage

Without limiting Contractor's indemnification of County, and in the performance of this Master Agreement and until all of its obligations pursuant to this Master Agreement have been met, Contractor must provide and maintain at its own expense insurance coverage satisfying the requirements specified in Subsection 8.24 of this Master Agreement. These minimum insurance coverage terms, types and limits (the “Required Insurance”) also are in addition to and separate from any other contractual obligation imposed upon Contractor pursuant to this Master Agreement. The County in no way warrants that the Required Insurance is sufficient to protect the Contractor for liabilities which may arise from or relate to this Master Agreement.

8.23.1 Evidence of Coverage and Notice to County

- Certificate(s) of insurance coverage (Certificate) satisfactory to County, and a copy of an Additional Insured endorsement confirming County and its Agents (defined below) has been given Insured status under the Contractor’s General Liability policy, must be delivered to County at the address shown below and provided prior to commencing services under this Master Agreement and upon award of a Service Requisition under this Master Agreement.
- Renewal Certificates must be provided to County not less than ten (10) days prior to Contractor’s policy expiration dates. The County reserves the right to obtain complete, certified copies of any required Contractor and/or Subcontractor insurance policies at any time.
- Certificates must identify all Required Insurance coverage types and limits specified herein, reference this Master Agreement by name or number, and be signed by an authorized representative of the insurer(s). The Insured party named on the Certificate must match the name of the Contractor identified as the contracting party in this Master Agreement. Certificates must provide the full name of each insurer providing coverage, its NAIC (National Association of Insurance Commissioners) identification number, its financial rating, the amounts of any policy deductibles or self-insured retentions exceeding fifty thousand ($50,000.00) dollars, and list any County required endorsement forms.

- Neither the County's failure to obtain, nor the County's receipt of, or failure to object to a non-complying insurance certificate or endorsement, or any other insurance documentation or information provided by the Contractor, its insurance broker(s) and/or insurer(s), will be construed as a waiver of any of the Required Insurance provisions.
- Certificates and copies of any required endorsements must be sent to:

  County of Los Angeles
  Department of Public Social Services
  Contract Administration and Monitoring Division – CSBG
  12900 Crossroads Parkway South
  City of Industry, CA 91746
  Attention: County Contract Administrator

- Contractor also must promptly report to County any injury or property damage accident or incident, including any injury to a Contractor employee occurring on County property, and any loss, disappearance, destruction, misuse, or theft of County property, monies or securities entrusted to Contractor. Contractor also must promptly notify County of any third-party claim or suit filed against Contractor or any of its Subcontractors which arises from or relates to this Master Agreement, and could result in the filing of a claim or lawsuit against Contractor and/or County.

8.23.2 Additional Insured Status and Scope of Coverage

The County of Los Angeles, its Special Districts, Elected Officials, Officers, Agents, Employees and Volunteers (collectively County and its Agents) must be provided additional insured status under Contractor's General Liability policy with respect to liability arising out of Contractor's ongoing and completed operations performed on behalf of the County. County and its Agents additional insured status must apply with respect to liability and defense of suits arising out of the Contractor's acts or omissions, whether such liability is attributable to the Contractor or to the County. The full policy limits and scope of protection also must apply to the County and its Agents as an additional insured, even if they exceed the County's minimum Required Insurance specifications herein. Use of an automatic additional insured endorsement form is acceptable providing it satisfies the Required Insurance provisions herein.

8.23.3 Cancellation of or Changes in Insurance

Contractor must provide County with, or Contractor's insurance policies must contain a provision that County will receive, written

notice of cancellation or any change in Required Insurance, including insurer, limits of coverage, term of coverage or policy period. The written notice must be provided to County at least ten (10) days in advance of cancellation for non-payment of premium and thirty (30) days in advance for any other cancellation or policy change. Failure to provide written notice of cancellation or any change in Required Insurance may constitute a material breach of the Master Agreement, in the sole discretion of the County, upon which the County may suspend or terminate this Master Agreement.

8.23.4 Failure to Maintain Insurance

Contractor's failure to maintain or to provide acceptable evidence that it maintains the Required Insurance will constitute a material breach of the Master Agreement, upon which County immediately may withhold payments due to Contractor, and/or suspend or terminate this Master Agreement. County, at its sole discretion, may obtain damages from Contractor resulting from said breach. Alternatively, the County may purchase the Required Insurance, and without further notice to Contractor, deduct the premium cost from sums due to Contractor or pursue Contractor reimbursement.

8.23.5 Insurer Financial Ratings

Coverage must be placed with insurers acceptable to the County with A.M. Best ratings of not less than A:VII unless otherwise approved by County.

8.23.6 Contractor’s Insurance Must Be Primary

Contractor’s insurance policies, with respect to any claims related to this Master Agreement, must be primary with respect to all other sources of coverage available to Contractor. Any County maintained insurance or self-insurance coverage must be in excess of and not contribute to any Contractor coverage.

8.23.7 Waivers of Subrogation

To the fullest extent permitted by law, the Contractor hereby waives its rights and its insurer(s)’ rights of recovery against County under all the Required Insurance for any loss arising from or relating to this Master Agreement. The Contractor must require its insurers to execute any waiver of subrogation endorsements which may be necessary to effect such waiver.

8.23.8 Subcontractor Insurance Coverage Requirements

Contractor must include all Subcontractors as insureds under Contractor’s own policies, or must provide County with each Subcontractor’s separate evidence of insurance coverage.

Contractor will be responsible for verifying each Subcontractor complies with the Required Insurance provisions herein, and must require that each Subcontractor name the County and Contractor as additional insureds on the Subcontractor's General Liability policy. Contractor must obtain County's prior review and approval of any Subcontractor request for modification of the Required Insurance.

8.23.9 Deductibles and Self-Insured Retentions (SIRs)

Contractor's policies will not obligate the County to pay any portion of any Contractor deductible or SIR. The County retains the right to require Contractor to reduce or eliminate policy deductibles and SIRs as respects the County, or to provide a bond guaranteeing Contractor's payment of all deductibles and SIRs, including all related claims investigation, administration and defense expenses. Such bond must be executed by a corporate surety licensed to transact business in the State of California.

8.23.10 Claims Made Coverage

If any part of the Required Insurance is written on a claims made basis, any policy retroactive date will precede the effective date of this Master Agreement. Contractor understands and agrees it will maintain such coverage for a period of not less than three (3) years following Master Agreement expiration, termination or cancellation.

8.23.11 Application of Excess Liability Coverage

Contractors may use a combination of primary, and excess insurance policies which provide coverage as broad as ("follow form" over) the underlying primary policies, to satisfy the Required Insurance provisions.

8.23.12 Separation of Insureds

All liability policies must provide cross-liability coverage as would be afforded by the standard ISO (Insurance Services Office, Inc.) separation of insureds provision with no insured versus insured exclusions or limitations.

8.23.13 Alternative Risk Financing Programs

The County reserves the right to review, and then approve, Contractor use of self-insurance, risk retention groups, risk purchasing groups, pooling arrangements and captive insurance to satisfy the Required Insurance provisions. The County and its Agents must be designated as an Additional Covered Party under any approved program.

8.23.14 County Review and Approval of Insurance Requirements

The County reserves the right to review and adjust the Required Insurance provisions, conditioned upon County's determination of changes in risk exposures.

8.24 Insurance Coverage

8.24.1 Commercial General Liability insurance (providing scope of coverage equivalent to ISO policy form CG 00 01), naming County and its Agents as an additional insured, with limits of not less than:

General Aggregate:	$2 million
Products/Completed Operations Aggregate:	$1 million
Personal and Advertising Injury:	$1 million
Each Occurrence:	$1 million

8.24.2 Automobile Liability insurance (providing scope of coverage equivalent to ISO policy form CA 00 01) with limits of not less than $1 million for bodily injury and property damage, in combined or equivalent split limits, for each single accident. Insurance must cover liability arising out of Contractor's use of autos pursuant to this Master Agreement, including owned, leased, hired, and/or non-owned autos, as each may be applicable.

8.24.3 Workers Compensation and Employers' Liability insurance or qualified self- insurance satisfying statutory requirements, which includes Employers' Liability coverage with limits of not less than $1 million per accident. If Contractor will provide leased employees, or, is an employee leasing or temporary staffing firm or a professional employer organization (PEO), coverage also must include an Alternate Employer Endorsement (providing scope of coverage equivalent to ISO policy form WC 00 03 01 A) naming the County as the Alternate Employer. The written notice must be provided to County at least ten (10) days in advance of cancellation for non-payment of premium and thirty (30) days in advance for any other cancellation or policy change. If applicable to Contractor's operations, coverage also must be arranged to satisfy the requirements of any federal workers or workmen's compensation law or any federal occupational disease law.

8.24.4 **Unique Insurance Coverage**

Contractor must provide and maintain at its own expense additional insurance as described below when applicable.

- Sexual Misconduct Liability

  Insurance covering actual or alleged claims for sexual misconduct and/or molestation with limits of not less than $2

million per claim and $2 million aggregate, and claims for negligent employment, investigation, supervision, training or retention of, or failure to report to proper authorities, a person(s) who committed any act of abuse, molestation, harassment, mistreatment or maltreatment of a sexual nature. This insurance coverage is required for Contractors providing services which involve the care or supervision of children, seniors and other vulnerable persons. This may include services such as childcare, foster care, group homes, emergency shelters, medical and/or mental health care service delivery, residential treatment, mentoring, schools, camp operations, school bus transport, and in-home services.

- Professional Liability/Errors and Omissions

  Insurance covering Contractor's liability arising from or related to this Master Agreement, with limits of not less than $1 million per claim and $3 million aggregate. Further, Contractor understands and agrees it must maintain such coverage for a period of not less than three (3) years following this Agreement's expiration, termination or cancellation. This insurance coverage is required for medical and legal services Contractors.

- Cyber Liability Insurance

  The Contractor must secure and maintain cyber liability insurance coverage with limits of $2 million per occurrence and in the aggregate during the term of the Master Agreement, including coverage for: network security liability; privacy liability; privacy regulatory proceeding, defense, response, expenses and fines; technology professional liability (errors and omissions); privacy breach expense reimbursement (liability arising from the loss or disclosure of County Information no matter how it occurs); system breach; denial or loss of service; introduction, implantation, or spread of malicious software code; unauthorized access to or use of computer systems; and Data/Information loss and business interruption; any other liability or risk that arises out of the Master Agreement. The Contractor must add the County as an additional insured to its cyber liability insurance policy and provide to the County certificates of insurance evidencing the foregoing upon the County's request. The procuring of the insurance described herein, or delivery of the certificates of insurance described herein, will not be construed as a limitation upon the Contractor's liability or as full performance of its indemnification obligations hereunder. No exclusion/ restriction for unencrypted portable devices/media may be on the policy.

8.25 Liquidated Damages

8.25.1 If, in the judgment of the Director, the Contractor is deemed to be non-compliant with the terms and obligations assumed hereby, the Director, or their designee, at their option, in addition to, or in lieu of, other remedies provided herein, may withhold the entire monthly payment or deduct pro rata from the Contractor's invoice for work not performed. A description of the work not performed and the amount to be withheld or deducted from payments to the Contractor from the County, will be forwarded to the Contractor by the Director, or their designee, in a written notice describing the reasons for said action.

8.25.2 If the Director determines that there are deficiencies in the performance of this Master Agreement that the Director or their designee, deems are correctable by the Contractor over a certain time span, the Director or their designee, will provide a written notice to the Contractor to correct the deficiency within specified time frames. Should the Contractor fail to correct deficiencies within said time frame, the Director may:

(a) Deduct from the Contractor's payment, pro rata, those applicable portions of the Monthly Contract Sum; and/or (b) Deduct liquidated damages. The parties agree that it will be impracticable or extremely difficult to fix the extent of actual damages resulting from the failure of the Contractor to correct a deficiency within the specified time frame. The parties hereby agree that under the current circumstances a reasonable estimate of such damages is one hundred dollars ($100) per day per infraction, or as may be specified in any Performance Requirements Summary (PRS) Charts in future Service Requisitions, and that the Contractor will be liable to the County for liquidated damages in said amount. Said amount will be deducted from the County's payment to the Contractor; and/or (c) Upon giving five (5) days' notice to the Contractor for failure to correct the deficiencies, the County may correct any and all deficiencies and the total costs incurred by the County for completion of the work by an alternate source, whether it be County forces or separate private contractor, will be deducted and forfeited from the payment to the Contractor from the County, as determined by the County.

8.25.3 The action noted in Paragraph 8.25.2 will not be construed as a penalty, but as adjustment of payment to the Contractor to recover the County cost due to the failure of the Contractor to complete or comply with the provisions of this Master Agreement.

8.25.4 This paragraph will not, in any manner, restrict or limit the County's right to damages for any breach of this Master

Agreement provided by law or as specified in the PRS or Paragraph 8.25.2, and will not, in any manner, restrict or limit the County's right to terminate this Master Agreement as agreed to herein.

8.26 Most Favored Public Entity

If the Contractor's prices decline, or should the Contractor at any time during the term of this Master Agreement provide the same goods or services under similar quantity and delivery conditions to the State of California or any county, municipality, or district of the State at prices below those set forth in this Master Agreement, then such lower prices will be immediately extended to the County.

8.27 Nondiscrimination and Affirmative Action

8.27.1 The Contractor certifies and agrees that all persons employed by it, its affiliates, subsidiaries, or holding companies are and will be treated equally without regard to or because of race, color, religion, ancestry, national origin, sex, age, physical or mental disability, marital status, or political affiliation, in compliance with all applicable federal and State anti-discrimination laws and regulations.

8.27.2 Contractor certifies to the County each of the following:

- That Contractor has a written policy statement prohibiting discrimination in all phases of employment.
- That Contractor periodically conducts a self-analysis or utilization analysis of its work force.
- That Contractor has a system for determining if its employment practices are discriminatory against protected groups.
- Where problem areas are identified in employment practices, the Contractor has a system for taking reasonable corrective action, to include establishment of goals or timetables.

8.27.3 The Contractor must take affirmative action to ensure that applicants are employed, and that employees are treated during employment, without regard to race, color, religion, ancestry, national origin, sex, age, physical or mental disability, marital status, or political affiliation, in compliance with all applicable federal and State anti-discrimination laws and regulations. Such action must include, but is not limited to: employment, upgrading, demotion, transfer, recruitment or recruitment advertising, layoff or termination, rates of pay or other forms of compensation, and selection for training, including apprenticeship.

8.27.4 The Contractor certifies and agrees that it will deal with its Subcontractors, bidders, or vendors without regard to or because

of race, color, religion, ancestry, national origin, sex, age, physical or mental disability, marital status, or political affiliation.

8.27.5 The Contractor certifies and agrees that it, its affiliates, subsidiaries, or holding companies will comply with all applicable federal and State laws and regulations to the end that no person will, on the grounds of race, color, religion, ancestry, national origin, sex, age, physical or mental disability, marital status, or political affiliation, be excluded from participation in, be denied the benefits of, or be otherwise subjected to discrimination under this Master Agreement or under any project, program, or activity supported by this Master Agreement.

8.27.6 The Contractor will allow County representatives access to the Contractor's employment records during regular business hours to verify compliance with the provisions of this Subsection 8.27 when so requested by the County.

8.27.7 If the County finds that any provisions of this Subsection 8.27 have been violated, such violation will constitute a material breach of this Master Agreement upon which the County may terminate or suspend this Master Agreement. While the County reserves the right to determine independently that the anti-discrimination provisions of this Master Agreement have been violated, in addition, a determination by the California Fair Employment and Housing Commission or the Federal Equal Employment Opportunity Commission that the Contractor has violated federal or State anti-discrimination laws or regulations will constitute a finding by the County that the Contractor has violated the anti-discrimination provisions of this Master Agreement.

8.27.8 The parties agree that in the event the Contractor violates any of the anti-discrimination provisions of this Master Agreement, the County will, at its sole option, be entitled to the sum of five hundred dollars ($500) for each such violation pursuant to California Civil Code Section 1671 as liquidated damages in lieu of terminating or suspending this Master Agreement.

8.28 Non Exclusivity

Nothing herein is intended nor will be construed as creating any exclusive arrangement with Contractor. This Master Agreement will not restrict the Department from acquiring similar, equal or like goods and/or services from other entities or sources.

8.29 Notice of Delays

Except as otherwise provided under this Master Agreement, when either party has knowledge that any actual or potential situation is delaying or threatens to delay the timely performance of this Master Agreement, that

party must, within one (1) business day, give notice thereof, including all relevant information with respect thereto, to the other party.

8.30 Notice of Disputes

The Contractor must bring to the attention of the County Contract Director and/or Supervising County Contract Administrator any dispute between the County and the Contractor regarding the performance of services as stated in this Master Agreement and subsequent Service Requisitions. If the County Contract Director or Supervising County Contract Administrator is not able to resolve the dispute, the DPSS Director or designee will resolve it.

8.31 Notice to Employees Regarding the Federal Earned Income Credit

The Contractor must notify its employees, and will require each Subcontractor to notify its employees, that they may be eligible for the Federal Earned Income Credit under the federal income tax laws. Such notice must be provided in accordance with the requirements set forth in Internal Revenue Service Notice No. 1015, which can be found at https://www.irs.gov/pub/irs-pdf/n1015.pdf.

8.32 Notice to Employees Regarding the Safely Surrendered Baby Law

The Contractor must notify and provide to its employees, and will require each Subcontractor to notify and provide to its employees, information regarding the Safely Surrendered Baby Law, its implementation in Los Angeles County, and where and how to safely surrender a baby. The information is set forth in Exhibit D, Safely Surrendered Baby Law of this Master Agreement. Additional information is available at:

https://lacounty.gov/residents/family-services/child-safety/safe-surrender/

8.33 Notices

All notices or demands required or permitted to be given or made under this Master Agreement must be in writing and will be hand delivered with signed receipt, emailed, or mailed by first-class registered or certified mail, postage prepaid, addressed to the parties as identified in Exhibits B (County's Administration) and C (Contractor's Administration). Addresses may be changed by either party giving ten (10) days' prior written notice thereof to the other party. The Director or their designee will have the authority to issue all notices or demands required or permitted by the County under this Master Agreement.

8.33.1 Notice of Meetings

Contractor must provide appropriate levels of staff at all meetings requested by the County. The County will give five (5) business days prior notice to the Contractor of the need to attend such meetings. Contractor may verbally request meetings with the County, as needed, with follow-up written notice five (5) business days in advance of the proposed meeting. The advance notice

requirement may be waived with the mutual consent of both Contractor and the County.

8.33.2 Notification to Contractor

The majority of the communications will be conducted via email. Contractor must ensure email is checked regularly.

8.34 Prohibition Against Inducement or Persuasion

Notwithstanding the above, the Contractor and the County agree that, during the term of this Master Agreement and for a period of one year thereafter, neither party will in any way intentionally induce or persuade any employee of one party to become an employee or agent of the other party. No bar exists against any hiring action initiated through a public announcement.

8.35 Public Records Act

8.35.1 Any documents submitted by Contractor; all information obtained in connection with the County's right to audit and inspect Contractor's documents, books, and accounting records pursuant to Subsection 8.37 (Record Retention and Inspection/Audit Settlement) of this Master Agreement; as well as those documents which were required to be submitted in response to the Request for RFSQ used in the solicitation process for this Master Agreement, become the exclusive property of the County. All such documents become a matter of public record and will be regarded as public records. Exceptions will be those elements in the California Government Code Section 7921 et seq. (Public Records Act) and which are marked "trade secret", "confidential", or "proprietary". The County will not in any way be liable or responsible for the disclosure of any such records including, without limitation, those so marked, if disclosure is required by law, or by an order issued by a court of competent jurisdiction.

8.35.2 In the event the County is required to defend an action on a Public Records Act request for any of the aforementioned documents, information, books, records, and/or contents of an SOQ marked "trade secret", "confidential", or "proprietary", the Contractor agrees to defend and indemnify the County from all costs and expenses, including reasonable attorney's fees, in action or liability arising under the Public Records Act.

8.36 Publicity

8.36.1 The Contractor must not disclose any details in connection with this Master Agreement to any person or entity except as may be otherwise provided hereunder or required by law. However, in recognizing the Contractor's need to identify its services and related clients to sustain itself, the County will not inhibit the Contractor from publishing its role under this Master Agreement

and any Service Requisition issued under this Master Agreement within the following conditions:

- The Contractor must develop all publicity material in a professional manner; and
- During the term of this Master Agreement, the Contractor must not, and will not authorize another to, publish or disseminate any commercial advertisements, press releases, feature articles, or other materials using the name of the County without the prior written consent of the County Contract Director. The County will not unreasonably withhold written consent.

8.36.2 The Contractor may, without the prior written consent of County, indicate in its proposals and sales materials that it has been awarded this Master Agreement with the County of Los Angeles, provided that the requirements of this Subsection 8.36 (Publicity) will apply.

8.37 Record Retention and Inspection-Audit Settlement

The Contractor must maintain accurate and complete financial records of its activities and operations relating to this Master Agreement in accordance with generally accepted accounting principles. The Contractor must also maintain accurate and complete employment and other records relating to its performance of this Master Agreement. The Contractor agrees that any State or federal agencies and the County, or its authorized representatives, will have access to and the right to examine, audit, excerpt, copy, or transcribe any pertinent transaction, activity, or record relating to this Master Agreement. All such material, including, but not limited to, all financial records, bank statements, cancelled checks or other proof of payment, timecards, sign-in/sign-out sheets and other time and employment records, and proprietary data and information, will be kept and maintained by the Contractor and will be made available to the County during the term of this Master Agreement and for a period of five (5) years thereafter unless the County's written permission is given to dispose of any such material prior to such time. All such material must be maintained by the Contractor at a location in Los Angeles County, provided that if any such material is located outside Los Angeles County, then, at the County's option, the Contractor will pay the County for travel, per diem, and other costs incurred by the County to examine, audit, excerpt, copy, or transcribe such material at such other location.

8.37.1 In the event that an audit of the Contractor is conducted specifically regarding this Master Agreement by any federal or State auditor, or by any auditor or accountant employed by the Contractor or otherwise, then the Contractor must file a copy of such audit report with the County's Auditor-Controller within thirty (30) days of the Contractor's receipt thereof, unless otherwise provided by

applicable federal or State law or under this Master Agreement. The County will make a reasonable effort to maintain the confidentiality of such audit report(s).

8.37.2 Failure on the part of the Contractor to comply with any of the provisions of this subsection will constitute a material breach of this Master Agreement upon which the County may terminate or suspend this Master Agreement.

8.37.3 If, at any time during the term of this Master Agreement or within five (5) years after the expiration or termination of this Master Agreement, representatives of the County may conduct an audit of the Contractor regarding the work performed under this Master Agreement, and if such audit finds that the County's dollar liability for any such work is less than payments made by the County to the Contractor, then the difference will be either: a) repaid by the Contractor to the County by cash payment upon demand or b) at the sole option of the County's Auditor-Controller, deducted from any amounts due to the Contractor from the County, whether under this Master Agreement or otherwise. If such audit finds that the County's dollar liability for such work is more than the payments made by the County to the Contractor, then the difference will be paid to the Contractor by the County by cash payment, provided that in no event will the County's maximum obligation for this Master Agreement exceed the funds appropriated by the County for the purpose of this Master Agreement.

8.38 Recycled Bond Paper

Consistent with the Board of Supervisors' policy to reduce the amount of solid waste deposited at the County landfills, the Contractor agrees to use recycled-content paper to the maximum extent possible on this Master Agreement.

8.39 Subcontracting

8.39.1 The requirements of this Master Agreement may not be subcontracted by the Contractor. Any attempt by the Contractor to subcontract may be deemed a material breach of this Master Agreement.

8.40 Termination for Breach of Warranty to Maintain Compliance with County's Child Support Compliance Program

Failure of the Contractor to maintain compliance with the requirements set forth in Subsection 8.13 (Contractor's Warranty of Adherence to County's Child Support Compliance Program), will constitute a default under this Master Agreement. Without limiting the rights and remedies available to the County under any other provision of this Master Agreement, failure of Contractor to cure such default within 90 calendar days of written notice will

be grounds upon which the County may terminate this Master Agreement pursuant to Subsection 8.42 (Termination for Default) and pursue debarment of Contractor, pursuant to County Code Chapter 2.202.

8.41 Termination for Convenience

8.41.1 County may terminate this Master Agreement, and any Service Requisition issued hereunder, in whole or in part, from time to time or permanently, when such action is deemed by the County, in its sole discretion, to be in its best interest. Termination of work hereunder will be effected by notice of termination to Contractor specifying the extent to which performance of work is terminated and the date upon which such termination becomes effective. The date upon which such termination becomes effective will be no less than ten (10) days after the notice is sent.

8.41.2 Upon receipt of a notice of termination and except as otherwise directed by the County, the Contractor must immediately:

- Stop work under the Service Requisition or under this Master Agreement, as identified in such notice;
- Transfer title and deliver to County all completed work and work in process; and
- Complete performance of such part of the work as would not have been terminated by such notice.

8.41.3 All material including books, records, documents, or other evidence bearing on the costs and expenses of the Contractor under this Master Agreement or Service Requisition must be maintained by the Contractor in accordance with Subsection 8.37 (Record Retention and Inspection/Audit Settlement).

8.42 Termination for Default

8.42.1 The County may, by written notice to the Contractor, terminate the whole or any part of this Master Agreement, if, in the judgment of the County Contract Director:

- Contractor has materially breached this Master Agreement;
- Contractor fails to timely provide and/or satisfactorily perform any task, deliverable, service, or other work required either under this Master Agreement or any Service Requisition issued hereunder; or
- Contractor fails to demonstrate a high probability of timely fulfillment of performance requirements of any Service Requisition issued under this Master Agreement, or of any obligations of this Master Agreement and in either case, fails to demonstrate convincing progress toward a cure within five (5) working days (or such longer period as the County may

authorize in writing) after receipt of written notice from the County specifying such failure.

8.42.2 In the event that the County terminates this Master Agreement in whole or in part as provided in Paragraph 8.42.1, the County may procure, upon such terms and in such manner as the County may deem appropriate, goods and services similar to those so terminated. The Contractor will be liable to the County for any and all excess costs incurred by the County, as determined by the County, for such similar goods and services. The Contractor will continue the performance of this Master Agreement to the extent not terminated under the provisions of this paragraph.

8.42.3 Except with respect to defaults of any Subcontractor, the Contractor will not be liable for any such excess costs of the type identified in Paragraph 8.42.2 if its failure to perform this Master Agreement, including any Service Requisition issued hereunder, arises out of causes beyond the control and without the fault or negligence of the Contractor. Such causes may include, but are not limited to: acts of God or of the public enemy, acts of the County in either its sovereign or contractual capacity, acts of federal or State governments in their sovereign capacities, fires, floods, epidemics, quarantine restrictions, strikes, freight embargoes, and unusually severe weather; but in every case, the failure to perform must be beyond the control and without the fault or negligence of the Contractor. If the failure to perform is caused by the default of a Subcontractor, and if such default arises out of causes beyond the control of both the Contractor and Subcontractor, and without the fault or negligence of either of them, the Contractor will not be liable for any such excess costs for failure to perform, unless the goods or services to be furnished by the Subcontractor were obtainable from other sources in sufficient time to permit the Contractor to meet the required performance schedule. As used in this Paragraph 8.42.3, the terms "Subcontractor" and "Subcontractors" mean Subcontractor(s) at any tier.

8.42.4 If, after the County has given notice of termination under the provisions of this Subsection 8.42, it is determined by the County that the Contractor was not in default under the provisions of this Subsection 8.42, or that the default was excusable under the provisions of Paragraph 8.42.3, the rights and obligations of the parties will be the same as if the notice of termination had been issued pursuant to Subsection 8.41 (Termination for Convenience).

8.42.5 The rights and remedies of the County provided in this Subsection 8.42 will not be exclusive and are in addition to any other rights and remedies provided by law or under this Master Agreement.

8.43 Termination for Improper Consideration

8.43.1 The County may, by written notice to the Contractor, immediately terminate the right of the Contractor to proceed under this Master Agreement if it is found that consideration, in any form, was offered or given by the Contractor, either directly or through an intermediary, to any County officer, employee, or agent with the intent of securing this Master Agreement or securing favorable treatment with respect to the award, amendment, or extension of the Master Agreement or the making of any determinations with respect to the Contractor's performance pursuant to the Master Agreement. In the event of such termination, the County will be entitled to pursue the same remedies against the Contractor as it could pursue in the event of default by the Contractor.

8.43.2 The Contractor must immediately report any attempt by a County officer, employee, or agent to solicit such improper consideration. The report must be made to the Los Angeles County Fraud Hotline at (800) 544-6861 or https://fraud.lacounty.gov/.

8.43.3 Among other items, such improper consideration may take the form of cash, discounts, services, the provision of travel or entertainment, or tangible gifts.

8.44 Termination for Insolvency

8.44.1 The County may terminate this Master Agreement forthwith in the event of the occurrence of any of the following:

- Insolvency of the Contractor. The Contractor will be deemed to be insolvent if it has ceased to pay its debts for at least sixty (60) days in the ordinary course of business or cannot pay its debts as they become due, whether or not a petition has been filed under the Federal Bankruptcy Code and whether or not the Contractor is insolvent within the meaning of the Federal Bankruptcy Code;
- The filing of a voluntary or involuntary petition regarding the Contractor under the Federal Bankruptcy Code;
- The appointment of a Receiver or Trustee for the Contractor; or
- The execution by the Contractor of a general assignment for the benefit of creditors.

8.44.2 The rights and remedies of the County provided in this Subsection 8.44 will not be exclusive and are in addition to any other rights and remedies provided by law or under this Master Agreement.

8.45 Termination for Non-Adherence of County Lobbyist Ordinance

The Contractor, and each County Lobbyist or County Lobbying firm as defined in County Code Section 2.160.010 retained by the Contractor, must fully comply with the County's Lobbyist Ordinance, County Code Section 2.160.010. Failure on the part of the Contractor or any County Lobbyist or County Lobbying firm retained by the Contractor to fully comply with the County's Lobbyist Ordinance will constitute a material breach of this Master Agreement, upon which the County may in its sole discretion, immediately terminate or suspend this Master Agreement.

8.46 Termination for Non-Appropriation of Funds

Notwithstanding any other provision of this Master Agreement, the County will not be obligated for the Contractor's performance hereunder or by any provision of this Master Agreement during any of the County's future fiscal years unless and until the County's Board of Supervisors appropriates funds for this Master Agreement in the County's Budget for each such future fiscal year. In the event that funds are not appropriated for this Master Agreement, then this Master Agreement will terminate as of December 31 of the last Calendar Year for which funds were appropriated. The County will notify the Contractor in writing of any such non-allocation of funds at the earliest possible date.

8.47 Validity

If any provision of this Master Agreement or the application thereof to any person or circumstance is held invalid, the remainder of this Master Agreement and the application of such provision to other persons or circumstances will not be affected thereby.

8.48 Waiver

No waiver by the County of any breach of any provision of this Master Agreement will constitute a waiver of any other breach or of such provision. Failure of the County to enforce at any time, or from time to time, any provision of this Master Agreement will not be construed as a waiver thereof. The rights and remedies set forth in this Subsection 8.48 will not be exclusive and are in addition to any other rights and remedies provided by law or under this Master Agreement.

8.49 Warranty Against Contingent Fees

8.49.1 The Contractor warrants that no person or selling agency has been employed or retained to solicit or secure this Master Agreement upon any agreement or understanding for a commission, percentage, brokerage, or contingent fee, excepting bona fide employees or bona fide established commercial or selling agencies maintained by the Contractor for the purpose of securing business.

8.49.2 For breach of this warranty, the County will have the right to terminate this Master Agreement and, at its sole discretion, deduct from the Master Agreement price or consideration, or otherwise recover, the full amount of such commission, percentage, brokerage, or contingent fee.

8.50 Warranty of Compliance with County's Defaulted Property Tax Reduction Program

Contractor acknowledges that County has established a goal of ensuring that all individuals and businesses that benefit financially from County through contract are current in paying their property tax obligations (secured and unsecured roll) in order to mitigate the economic burden otherwise imposed upon County and its taxpayers.

Unless Contractor qualifies for an exemption or exclusion, Contractor warrants and certifies that to the best of its knowledge it is now in compliance, and during the term of this Master Agreement will maintain compliance, with Los Angeles County Code Chapter 2.206.

8.51 Termination for Breach of Warranty to Maintain Compliance with County's Defaulted Property Tax Reduction Program

Failure of Contractor to maintain compliance with the requirements set forth in Subsection 8.50 (Warranty of Compliance with County's Defaulted Property Tax Reduction Program) will constitute default under this Master Agreement. Without limiting the rights and remedies available to County under any other provision of this Master Agreement, failure of Contractor to cure such default within ten (10) days of notice will be grounds upon which County may terminate this Master Agreement and/or pursue debarment of Contractor, pursuant to Los Angeles County Code Chapter 2.206.

8.52 Time off For Voting

The Contractor must notify its employees, and must require each Subcontractor to notify and provide to its employees, information regarding the time off for voting law (Elections Code Section 14000). Not less than ten (10) days before every statewide election, every Contractor and Subcontractors must keep posted conspicuously at the place of work, if practicable, or elsewhere where it can be seen as employees come or go to their place of work, a notice setting forth the provisions of Section 14000.

8.53 Compliance with County's Zero Tolerance Policy on Human Trafficking

Contractor acknowledges that the County has established a Zero Tolerance Policy on Human Trafficking prohibiting Contractors from engaging in human trafficking.

If a Contractor or member of Contractor's staff is convicted of a human trafficking offense, the County will require that the Contractor or member of Contractor's staff be removed immediately from performing services under the Master Agreement. County will not be under any obligation to disclose

confidential information regarding the offenses other than those required by law.

Disqualification of any member of Contractor's staff pursuant to this Subsection will not relieve Contractor of its obligation to complete all work in accordance with the terms and conditions of this Master Agreement.

8.54 Intentionally Omitted

8.55 Compliance with Fair Chance Employment Hiring Practices

Contractor, and its Subcontractors, must comply with fair chance employment hiring practices set forth in California Government Code Section 12952, Contractor's violation of this Subsection of the Contract may constitute a material breach of the Master Agreement. In the event of such material breach, County may, in its sole discretion, terminate the Master Agreement.

8.56 Compliance with the County Policy of Equity

The Contractor acknowledges that the County takes its commitment to preserving the dignity and professionalism of the workplace very seriously, as set forth in the County Policy of Equity (CPOE) (https://ceop.lacounty.gov/). The contractor further acknowledges that the County strives to provide a workplace free from discrimination, harassment, retaliation and inappropriate conduct based on a protected characteristic, and which may violate the CPOE. The Contractor, its employees and Subcontractors acknowledge and certify receipt and understanding of the CPOE. Failure of the Contractor, its employees or its Subcontractors to uphold the County's expectations of a workplace free from harassment and discrimination, including inappropriate conduct based on a protected characteristic, may subject the Contractor to termination of contractual agreements as well as civil liability.

8.57 Prohibition from Participation in Future Solicitation(s)

A Proposer, or a Contractor or its subsidiary or Subcontractor ("Proposer/Contractor"), is prohibited from submitting a bid or proposal in a County solicitation if the Proposer/Contractor has provided advice or consultation for the solicitation. A Proposer/Contractor is also prohibited from submitting a bid or proposal in a County solicitation if the Proposer/Contractor has developed or prepared any of the solicitation materials on behalf of the County. A violation of this provision will result in the disqualification of the Contractor/Proposer from participation in the County solicitation or the termination or cancellation of any resultant County contract.

8.58 Injury and Illness Prevention Program

Contractor will be required to comply with the State of California's Cal OSHA's regulations. California Code of Regulations Title 8 Section 3203 requires all California employers to have a written, effective Injury and

Illness Prevention Program (IIPP) that addresses hazards pertaining to the particular workplace covered by the program.

8.59 Campaign Contribution Prohibition Following Final Decision in Master Agreement Proceeding

Pursuant to Government Code Section 84308, Contractor and its Subcontractors, are prohibited from making a contribution of more than $250 to a County officer for twelve (12) months after the date of the final decision in the proceeding involving this Master Agreement. Failure to comply with the provisions of Government Code Section 84308 and of this Subsection, may be a material breach of this Master Agreement as determined in the sole discretion of the County.

9.0 UNIQUE TERMS AND CONDITIONS

9.1 Health Insurance Portability and Accountability Act of 1996 (HIPAA)

9.1.1 Contractor expressly acknowledges and agrees that the provision of services under this Agreement does not require or permit access by Contractor or any of its officers, employees, or agents, to any patient medical records/patient information. Accordingly, Contractor must instruct its officers, employees, and agents that they are not to pursue, or gain access to, patient medical records/patient information for any reason whatsoever.

9.1.2 Notwithstanding the forgoing, the parties acknowledge that in the course of the provision of services hereunder, Contractor or its officers, employees, and agents, may have inadvertent access to patient medical records/patient information. Contractor understands and agrees that neither it nor its officers, employees, or agents, are to take advantage of such access for any purpose whatsoever.

9.1.3 Additionally, in the event of such inadvertent access, Contractor and its officers, employees, and agents, must maintain the confidentiality of any information obtained and must notify the Director that such access has been gained immediately, or upon the first reasonable opportunity to do so. In the event of any access, whether inadvertent or intentional, Contractor must indemnify, defend, and hold harmless County, its officers, employees, and agents, from and against any and all liability, including but not limited to, actions, claims, costs, demands, expenses, and fees (including attorney and expert witness fees) arising from or connected with Contractor's or its officers', employees', or agents', access to patient medical records/patient information. Contractor agrees to provide appropriate training to its employees regarding their obligations as described hereinabove.

9.2 Contractor's Charitable Activities Compliance

The Supervision of Trustees and Fundraisers for Charitable Purposes Act regulates entities receiving or raising charitable contributions. The "Nonprofit Integrity Act of 2004" (SB 1262, Chapter 919) increased Charitable Purposes Act requirements. By requiring Contractors to complete Exhibit F (Charitable Contributions Certification), the County seeks to ensure that all County Contractors which receive or raise charitable contributions comply with California law in order to protect the County and its taxpayers. A Contractor which receives or raises charitable contributions without complying with its obligations under California law commits a material breach subjecting it to either Master Agreement termination or debarment proceedings or both. (County Code Chapter 2.202)

9.3 Social Enterprise (SE) Preference Program

9.3.1 This Master Agreement is subject to the provisions of the County's ordinance entitled SE Preference Program, as codified in Chapter 2.205 of the Los Angeles County Code.

9.3.2 Contractor must not knowingly and with the intent to defraud, fraudulently obtain, retain, attempt to obtain or retain, or aid another in fraudulently obtaining or retaining or attempting to obtain or retain certification as a SE.

9.3.3 Contractor must not willfully and knowingly make a false statement with the intent to defraud, whether by affidavit, report, or other representation, to a County official or employee for the purpose of influencing the certification or denial of certification of any entity as a SE.

9.3.4 If Contractor has obtained County certification as a SE by reason of having furnished incorrect supporting information or by reason of having withheld information, and which knew, or should have known, the information furnished was incorrect or the information withheld was relevant to its request for certification, and which by reason of such certification has been awarded this Master Agreement to which it would not otherwise have been entitled, Contractor will:

- Pay to the County any difference between the Master Agreement amount and what the County's costs would have been if the Master Agreement had been properly awarded;
- In addition to the amount described in subdivision (1) above, the Contractor will be assessed a penalty in an amount of not more than ten percent (10%) of the amount of the Master Agreement; and
- Be subject to the provisions of Chapter 2.202 of the Los Angeles County Code (Determinations of Contractor Non-responsibility and Contractor Debarment).

The above penalties will also apply to any entity that has previously obtained proper certification, however, as a result of a change in their status would no longer be eligible for certification, and fails to notify the Department of Consumer and Business Affairs of this information prior to responding to a solicitation or accepting a Master Agreement award.

9.4 Disabled Veteran Business Enterprise (DVBE) Preference Program

9.4.1 This Master Agreement is subject to the provisions of the County's ordinance entitled DVBE Preference Program, as codified in Chapter 2.211 of the Los Angeles County Code.

9.4.2 Contractor must not knowingly and with the intent to defraud, fraudulently obtain, retain, attempt to obtain or retain, or aid another in fraudulently obtaining or retaining or attempting to obtain or retain certification as a DVBE.

9.4.3 Contractor must not willfully and knowingly make a false statement with the intent to defraud, whether by affidavit, report, or other representation, to a County official or employee for the purpose of influencing the certification or denial of certification of any entity as a DVBE.

9.4.4 If Contractor has obtained certification as a DVBE by reason of having furnished incorrect supporting information or by reason of having withheld information, and which knew, or should have known, the information furnished was incorrect or the information withheld was relevant to its request for certification, and which by reason of such certification has been awarded this Master Agreement to which it would not otherwise have been entitled, Contractor will:

- Pay to the County any difference between the Master Agreement amount and what the County's costs would have been if the Master Agreement had been properly awarded;
- In addition to the amount described in subdivision (1) above, the Contractor will be assessed a penalty in an amount of not more than ten percent (10%) of the amount of the Master Agreement; and
- Be subject to the provisions of Chapter 2.202 of the Los Angeles County Code (Determinations of Contractor Non-responsibility and Contractor Debarment).

Not withstanding any other remedies in this Master Agreement, the above penalties will also apply to any business that has previously obtained proper certification, however, as a result of a change in their status would no longer be eligible for certification, and fails to notify the State and the Department of Consumer and

Business Affairs of this information prior to responding to a solicitation or accepting a Master Agreement award.

9.5 Certification Regarding Debarment, Suspension, Ineligibility and Voluntary Exclusion - Lower Tier Covered Transactions (45 C.F.R. Part 76)

9.5.1 Contractor hereby acknowledges that County is prohibited from contracting with and making sub-awards to parties that are suspended, debarred, ineligible, or excluded or whose principals are suspended, debarred, ineligible, or excluded from securing federally funded contracts.

9.5.2 By executing this Master Agreement, Contractor certifies that neither it nor any of its owners, officers, partners, directors or other principals is currently suspended, debarred, ineligible, or excluded from securing federally funded contracts. Further, by executing this Master Agreement, Contractor certifies that, to its knowledge, none of its Subcontractors, at any tier, or any owner, officer, partner, director or other principal of any Subcontractors is currently suspended, debarred, ineligible, or excluded from securing federally funded contracts. Contractor must immediately notify County in writing, during the term of this Master Agreement, should it or any of its Subcontractors or any principals of either be suspended, debarred, ineligible, or excluded from securing federally funded contracts. Failure of Contractor to comply with this provision will constitute a material breach of this Master Agreement upon which County may immediately terminate or suspend this Master Agreement.

9.6 Child/Elder Abuse and Fraud Reporting

9.6.1 Contractor staff working under the terms of this Master Agreement and subsequent Service Requisitions must comply with California Penal Code (hereinafter “PC”) Section 11164 et seq. and must report all known and suspected instances of child abuse to an appropriate child protective agency, as mandated by these code sections.

9.6.2 Child abuse reports must be made by telephone to the Department of Children and Family Services hotline at (800) 540-4000 immediately, and must submit all required information, in accordance with the PC Sections 11166 and 11167, within 36 hours to: https://mandreptla.org/cars.web/.

9.6.3 Contractor staff working on this Master Agreement and subsequent Service Requisitions must comply with California W&IC, Section 15600 et seq. and must report all known or suspected instances of physical or mental/emotional abuse of elders and dependent adults either to the appropriate County adult

protective services agency or to a local law enforcement agency, as mandated by these code sections.

9.6.4 Elder abuse reports must be made by telephone to the Los Angeles County Aging & Disabilities Department hotline at (877) 477-3646 [(877) 4R-SENIORS] and must submit all required information, in accordance with the W&IC Sections 15630, 15633, and 15633.5.

9.6.5 Contractor staff working under the terms of this Master Agreement and subsequent Service Requisitions must also immediately report all suspected or actual welfare fraud situations to the County via the 24-hour Central DPSS Fraud Reporting Line at (800) 349-9970, or the Employee Fraud Hotline (800) 544-6861, or California State Fraud Hotline (800) 822-6222.

9.7 Government Observations

Contractor must permit all authorized federal, State, County and/or research personnel, in addition to departmental contracting staff, to observe performance, activities, or review documents required under this Contract at any time during normal working hours. However, these personnel may not unreasonably interfere with Contractor performance.

9.8 Shred Confidential Documents

Contractor must ensure that all confidential documents/papers, as defined under State law (including but not limited to Welfare & Institutions Code Sections 10850, 17006) relating to this Master Agreement must be shredded and not discarded in trash containers when Contractor disposes of these documents/papers. All documents/papers to be shredded are to be placed in a locked or secured container/bin/box and labeled “shred” until they are destroyed. No confidential documents/papers are to be recycled. Documents for record and retention purposes in accordance with Subsection 8.37, of this Master Agreement are to be maintained for a period of five (5) years after the term of this Master Agreement or for a period of five (5) years following the last date of service or until all audits started are completed, whichever is later.

9.9 System for Award Management

Per Title 2 e-CFR 200.212, all Contractors, their principals or affiliates or any Subcontractors that receive federal funds must be in good standing with the federal government. As such, Contractor **must** ensure that their System for Award Management registration remains active for the duration of the Master Agreement term.

9.10 Privacy and Security Agreement

The County and Contractor agree to review and comply with applicable privacy and security requirements [Exhibit H-1, 2019 CDSS Privacy and Security Agreement; Exhibit H-2, DHCS 2024 Medi-Cal Privacy and

Security Agreement; and Exhibit H-3, Electronic Information Exchange Security Requirements and Procedures for State and Local Agencies Exchanging Electronic Information with the SSA (TSSR)] in order to ensure the privacy and security of the CalSAWS, Social Security Administration (SSA), Medi-Cal Eligibility Data System (MEDS), Applicant Income, Eligibility Verification System (IEVS), and Personally Identifiable Information (PII) data that is covered by these agreements and accessed or provided through DPSS.

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

DPSS **Department Information Security Officer**	**DPSS** **County Contract Administrator**
Department of Public Social Services Bureau of Technology Services Information Technology Security Office 12851 Crossroads Parkway South City of Industry, CA 91746-3411 Email: ITSO@dpss.lacounty.gov Telephone: (562) 551-3487	Please refer to Exhibit B for CCA contact information.
The preferred method of communication is email, when available. Do not include any PII unless requested by CAM or the DPSS Department Information Security Officer.	The preferred method of communication is email, when available. Do not include any Medi-Cal PII unless requested by DPSS Contract Administration and Monitoring Division.

10.0 Survival

In addition to any terms and conditions of this Master Agreement that expressly survive expiration or termination of this Master Agreement by their terms, the following provisions will survive the expiration or termination of this Master Agreement for any reason:

Section 1.0 (Applicable Documents)

Section 2.0 (Definitions)

Section 3.0	(Work)
Subsection 5.3	(No Payment for Services Provided Following Expiration/Termination of Master Agreement)
Subsection 7.6	(Confidentiality)
Subsection 8.1	(Amendments and Change Notices)
Subsection 8.2	(Assignment and Delegation/Mergers or Acquisitions)
Subsection 8.18	(Fair Labor Standards)
Subsection 8.19	(Force Majeure)
Subsection 8.20	(Governing Law, Jurisdiction, and Venue)
Subsection 8.22	(Indemnification)
Subsection 8.23	(General Provisions for all Insurance Coverage)
Subsection 8.24	(Insurance Coverage)
Subsection 8.25	(Liquidated Damages)
Subsection 8.33	(Notices)
Subsection 8.37	(Record Retention and Inspection-Audit Settlement)
Subsection 8.41	(Termination for Convenience)
Subsection 8.42	(Termination for Default)
Subsection 8.47	(Validity)
Subsection 8.48	(Waiver)
Subsection 8.57	(Prohibition from Participation in Future Solicitation(s))
Subsection 8.59	(Campaign Contribution Prohibition Following Final Decision in Master Agreement Proceeding)
Subsection 9.8	(Shred Confidential Documents)
Section 10.0	(Survival)

AUTHORIZATION OF MASTER AGREEMENT FOR

COMMUNITY SERVICE BLOCK GRANT PROGRAM SERVICES

IN WITNESS WHEREOF, the Board of Supervisors of the County of Los Angeles has caused this Master Agreement to be executed by the Director of the Department of Public Social Services or designee and approved by County Counsel, and Contractor has caused this Master Agreement to be executed in its behalf by its duly authorized officer, this _____ day of _____, 20___.

COUNTY OF LOS ANGELES

By:_____
Jackie Contreras, Ph.D., Director
Department of Public Social Services

Date: _____

By:_____
Contractor

Signed: _____

Printed Name: _____

Title: _____

APPROVED AS TO FORM:

BY THE OFFICE OF COUNTY COUNSEL
Dawyn R. Harrison, County Counsel
Melinda White-Svec, Deputy County Counsel

Form Community Services Block Grant Program Master Agreement was Submitted and Approved as to Form. Documentation on File.

SCOPE OF SERVICES

Contractor is pre-qualified for the following Core Service Categories and Supervisorial Districts:

	Supervisorial Districts				
	1	**2**	**3**	**4**	**5**
Child and Family Development Services					
Domestic Violence Services					
Emergency Services					
Employment Services					
Legal Services					
Senior and/or Disabled Adult Services					

COUNTY'S ADMINISTRATION

MASTER AGREEMENT NO. Click or tap here to enter text.

COUNTY CONTRACT DIRECTOR:

Name: Click or tap here to enter text.
Title: Click or tap here to enter text.
Address: Click or tap here to enter text.
Click or tap here to enter text.
Telephone: Click or tap here to enter text.
E-mail Address: Click or tap here to enter text.

SUPERVISING COUNTY CONTRACT ADMINISTRATOR:

Name: Click or tap here to enter text.
Title: Click or tap here to enter text.
Address: Click or tap here to enter text.
Click or tap here to enter text.
Telephone: Click or tap here to enter text.
E-mail Address: Click or tap here to enter text.

COUNTY CONTRACT ADMINISTRATOR:

Name: Click or tap here to enter text.
Title: Click or tap here to enter text.
Address: Click or tap here to enter text.
Click or tap here to enter text.
Telephone: Click or tap here to enter text.
E-mail Address: Click or tap here to enter text.

COUNTY PROGRAM MONITOR (CPM):

Name: Click or tap here to enter text.
Title: Click or tap here to enter text.
Address: Click or tap here to enter text.
Click or tap here to enter text.
Telephone: Click or tap here to enter text.
E-mail Address: Click or tap here to enter text.

COUNTY CONTRACT PROGRAM MANAGER:

Name: Click or tap here to enter text.
Title: Click or tap here to enter text.
Address: Click or tap here to enter text.
Click or tap here to enter text.
Telephone: Click or tap here to enter text.
E-mail Address: Click or tap here to enter text.

CONTRACTOR'S ADMINISTRATION

CONTRACTOR'S NAME: Click or tap here to enter text.

MASTER AGREEMENT NO. Click or tap here to enter text.

CONTRACTOR'S CONTRACT MANAGER:

Name: Click or tap here to enter text.
Title: Click or tap here to enter text.
Address: Click or tap here to enter text.
Click or tap here to enter text.
Telephone: Click or tap here to enter text.
E-mail Address: Click or tap here to enter text.

CONTRACTOR'S AUTHORIZED OFFICIAL(S):

Name: Click or tap here to enter text.
Title: Click or tap here to enter text.
Address: Click or tap here to enter text.
Click or tap here to enter text.
Telephone: Click or tap here to enter text.
E-mail Address: Click or tap here to enter text.

Name: Click or tap here to enter text.
Title: Click or tap here to enter text.
Address: Click or tap here to enter text.
Click or tap here to enter text.
Telephone: Click or tap here to enter text.
E-mail Address: Click or tap here to enter text.

NOTICES TO CONTRACTOR:

Name: Click or tap here to enter text.
Title: Click or tap here to enter text.
Address: Click or tap here to enter text.
Click or tap here to enter text.
Telephone: Click or tap here to enter text.
E-mail Address: Click or tap here to enter text.


THERE'S A BETTER CHOICE.
SAFELY SURRENDER YOUR BABY.
Any fire station. Any hospital. Any time.
1.877.222.9723
BabySafeLA.org
No shame | No blame | No names
21
FIRE STATION
98

Some parents of newborns can find themselves in difficult circumstances. Sadly, babies are sometimes harmed or abandoned by parents who feel that they're not ready or able to raise a child. Many of these mothers or fathers are afraid and don't know where to turn for help.

This is why California has a Safely Surrendered Baby Law, which gives parents the choice to legally leave their baby at any hospital or fire station in Los Angeles County.

FIVE THINGS YOU NEED TO KNOW ABOUT BABY SAFE SURRENDER

1. Your newborn can be surrendered at any hospital or fire station in Los Angeles County up to 72 hours after birth.
2. You must leave your newborn with a fire station or hospital employee.
3. You don't have to provide your name.
4. You will only be asked to voluntarily provide a medical history.
5. You have 14 days to change your mind; a matching bracelet (parent) and anklet (baby) are provided to assist you if you change your mind.

No shame | No blame | No names

BabySafeLA.org

ABOUT THE BABY SAFE SURRENDER PROGRAM

In 2002, a task force was created under the guidance of the Children's Planning Council to address newborn abandonment and to develop a strategic plan to prevent this tragedy.

Los Angeles County has worked hard to ensure that the Safely Surrendered Baby Law prevents babies from being abandoned. We're happy to report that this law is doing exactly what it was designed to do: save the lives of innocent babies. Visit BabySafeLA.org to learn more.

No shame | No blame | No names

ANY FIRE STATION.
ANY HOSPITAL.
ANY TIME.

1.877.222.9723
BabySafeLA.org

THERE'S A BETTER CHOICE.
SAFELY SURRENDER YOUR BABY.

BabySafeLA.org

No shame | No blame | No names

FROM SURRENDER TO ADOPTION: ONE BABY'S STORY

Los Angeles County firefighter Ted and his wife Becki were already parents to two boys. But when they got the call asking if they would be willing to care for a premature baby girl who'd been safely surrendered at a local hospital, they didn't hesitate.

Baby Jenna was tiny, but Ted and Becki felt lucky to be able to take her home. "We had always wanted to adopt," Ted says, "but taking home a vulnerable safely surrendered baby was even better. She had no one, but now she had us. And, more importantly, we had her."

Baby Jenna has filled the longing Ted and Becki had for a daughter—and a sister for their boys. Because her birth parent safely surrendered her when she was born, Jenna is a thriving young girl growing up in a stable and loving family.

ANSWERS TO YOUR QUESTIONS

Who is legally allowed to surrender the baby?
Anyone with lawful custody can drop off a newborn within the first 72 hours of birth.

Do you need to call ahead before surrendering a baby?
No. A newborn can be surrendered anytime, 24 hours a day, 7 days a week, as long as the parent or guardian surrenders the child to an employee of the hospital or fire station.

What information needs to be provided?
The surrendering adult will be asked to fill out a medical history form, which is useful in caring for the child. The form can be returned later and includes a stamped return envelope. No names are required.

What happens to the baby?
After a complete medical exam, the baby will be released and placed in a safe and loving home, and the adoption process will begin.

What happens to the parent or surrendering adult?
Nothing. They may leave at any time after surrendering the baby.

How can a parent get a baby back?
Parents who change their minds can begin the process of reclaiming their baby within 14 days by calling the Los Angeles County Department of Children and Family Services at (800) 540-4000.

If you're unsure of what to do:
You can call the hotline 24 hours a day, 7 days a week and anonymously speak with a counselor about your options or have your questions answered.

1.877.222.9723 or BabySafeLA.org
English, Spanish and 140 other languages spoken.

CONTRACTOR ACKNOWLEDGEMENT AND CONFIDENTIALITY AGREEMENT

(Note: This certification is to be executed and returned to County with Contractor's executed Master Agreement. Work cannot begin on the Service Requisition until County receives this executed document.)

Contractor Name: _____

Master Agreement No.: _____

GENERAL INFORMATION:

The Contractor referenced above has entered into a Master Agreement with the County of Los Angeles to provide certain services to the County. The County requires the Corporation to sign this Contractor Acknowledgement and Confidentiality Agreement.

CONTRACTOR ACKNOWLEDGEMENT:

Contractor understands and agrees that the Contractor employees, consultants, Outsourced Vendors and independent contractors (Contractor's Staff) that will provide services in the above referenced agreement are Contractor's sole responsibility. Contractor understands and agrees that Contractor's Staff must rely exclusively upon Contractor for payment of salary and any and all other benefits payable by virtue of Contractor's Staff's performance of work under the above-referenced Master Agreement.

Contractor understands and agrees that Contractor's Staff are not employees of the County of Los Angeles for any purpose whatsoever and that Contractor's Staff do not have and will not acquire any rights or benefits of any kind from the County of Los Angeles by virtue of my performance of work under the above-referenced Master Agreement. Contractor understands and agrees that Contractor's Staff will not acquire any rights or benefits from the County of Los Angeles pursuant to any agreement between any person or entity and the County of Los Angeles.

CONFIDENTIALITY AGREEMENT:

Contractor and Contractor's Staff may be involved with work pertaining to services provided by the County of Los Angeles and, if so, Contractor and Contractor's Staff may have access to confidential data and information pertaining to persons and/or entities receiving services from the County. In addition, Contractor and Contractor's Staff may also have access to proprietary information supplied by other vendors doing business with the County of Los Angeles. The County has a legal obligation to protect all such confidential data and information in its possession, especially data and information concerning health, criminal, and welfare recipient records. Contractor and Contractor's Staff understand that if they are involved in County work, the County must ensure that Contractor and Contractor's Staff, will protect the confidentiality of such data and information. Consequently, Contractor must sign this Confidentiality Agreement as a condition of work to be provided by Contractor's Staff for the County.

Contractor and Contractor's Staff hereby agrees that they will not divulge to any unauthorized person any data or information obtained while performing work pursuant to the above-referenced Master Agreement between Contractor and the County of Los Angeles. Contractor and Contractor's Staff agree to forward all requests for the release of any data or information received to County's Project Manager.

Contractor and Contractor's Staff agree to keep confidential all health, criminal, and welfare recipient records and all data and information pertaining to persons and/or entities receiving services from the County, design concepts, algorithms, programs, formats, documentation, Contractor proprietary information and all other original materials produced, created, or provided to Contractor and Contractor's Staff under the above-referenced Master Agreement. Contractor and Contractor's Staff agree to protect these confidential materials against disclosure to other than Contractor or County employees who have a need to know the information. Contractor and Contractor's Staff agree that if proprietary information supplied by other County vendors is provided to me during this employment, Contractor and Contractor's Staff must keep such information confidential.

Contractor and Contractor's Staff agree to report any and all violations of this agreement by Contractor and Contractor's Staff and/or by any other person of whom Contractor and Contractor's Staff become aware.

Contractor and Contractor's Staff acknowledge that violation of this agreement may subject Contractor and Contractor's Staff to civil and/or criminal action and that the County of Los Angeles may seek all possible legal redress.

SIGNATURE: _____ DATE: _____

PRINTED NAME: _____

POSITION: _____

CONTRACTOR EMPLOYEE ACKNOWLEDGEMENT AND CONFIDENTIALITY AGREEMENT

(Note: This certification is to be executed and returned to County with Contractor's executed Service Requisition. Work cannot begin on the Service Requisition until County receives this executed document.)

Contractor Name: _____ Employee Name: _____

Service Requisition No.: _____ Master Agreement No.: _____

GENERAL INFORMATION:

Your employer referenced above has entered into a Master Agreement with the County of Los Angeles to provide certain services to the County. The County requires your signature on this Contractor Employee Acknowledgement and Confidentiality Agreement.

EMPLOYEE ACKNOWLEDGEMENT:

I understand and agree that the Contractor referenced above is my sole employer for purposes of the above-referenced Master Agreement. I understand and agree that I must rely exclusively upon my employer for payment of salary and any and all other benefits payable to me or on my behalf by virtue of my performance of work under the above-referenced Master Agreement.

I understand and agree that I am not an employee of the County of Los Angeles for any purpose whatsoever and that I do not have and will not acquire any rights or benefits of any kind from the County of Los Angeles by virtue of my performance of work under the above-referenced Master Agreement. I understand and agree that I do not have and will not acquire any rights or benefits from the County of Los Angeles pursuant to any agreement between any person or entity and the County of Los Angeles.

I understand and agree that I may be required to undergo a background and security investigation(s). I understand and agree that my continued performance of work under the above-referenced Master Agreement is contingent upon my passing, to the satisfaction of the County, any and all such investigations. I understand and agree that my failure to pass, to the satisfaction of the County, any such investigation will result in my immediate release from performance under this and/or any future Master Agreement.

CONFIDENTIALITY AGREEMENT:

I may be involved with work pertaining to services provided by the County of Los Angeles and, if so, I may have access to confidential data and information pertaining to persons and/or entities receiving services from the County. In addition, I may also have access to proprietary information supplied by other vendors doing business with the County of Los Angeles. The County has a legal obligation to protect all such confidential data and information in its possession, especially data and information concerning health, criminal, and welfare recipient records. I understand that if I am involved in County work, the County must ensure that I, too, will protect the confidentiality of such data and information. Consequently, I understand that I must sign this agreement as a condition of my work to be provided by my employer for the County. I have read this agreement and have taken due time to consider it prior to signing.

I hereby agree that I will not divulge to any unauthorized person any data or information obtained while performing work pursuant to the above-referenced Master Agreement between my employer and the County of Los Angeles. I agree to forward all requests for the release of any data or information received by me to my immediate supervisor.

I agree to keep confidential all health, criminal, and welfare recipient records and all data and information pertaining to persons and/or entities receiving services from the County, design concepts, algorithms, programs, formats, documentation, Contractor proprietary information and all other original materials produced, created, or provided to or by me under the above-referenced Master Agreement. I agree to protect these confidential materials against disclosure to other than my employer or County employees who have a need to know the information. I agree that if proprietary information supplied by other County vendors is provided to me during this employment, I must keep such information confidential.

I agree to report to my immediate supervisor any and all violations of this agreement by myself and/or by any other person of whom I become aware. I agree to return all confidential materials to my immediate supervisor upon completion of this Master Agreement or termination of my employment with my employer, whichever occurs first.

SIGNATURE: _____ DATE: _____

PRINTED NAME: _____

POSITION: _____

CONTRACTOR NON-EMPLOYEE ACKNOWLEDGEMENT AND CONFIDENTIALITY AGREEMENT

(Note: This certification is to be executed and returned to County with Contractor's executed Service Requisition. Work cannot begin on the Service Requisition until County receives this executed document.)

Contractor Name: _____ Non-Employee Name: _____

Service Requisition No.: _____ Master Agreement No.: _____

GENERAL INFORMATION:

The Contractor referenced above has entered into a Master Agreement with the County of Los Angeles to provide certain services to the County. The County requires your signature on this Contractor Non-Employee Acknowledgement and Confidentiality Agreement.

NON-EMPLOYEE ACKNOWLEDGEMENT:

I understand and agree that the Contractor referenced above has exclusive control for purposes of the above-referenced Master Agreement. I understand and agree that I must rely exclusively upon the Contractor referenced above for payment of salary and any and all other benefits payable to me or on my behalf by virtue of my performance of work under the above-referenced Master Agreement.

I understand and agree that I am not an employee of the County of Los Angeles for any purpose whatsoever and that I do not have and will not acquire any rights or benefits of any kind from the County of Los Angeles by virtue of my performance of work under the above-referenced Master Agreement. I understand and agree that I do not have and will not acquire any rights or benefits from the County of Los Angeles pursuant to any agreement between any person or entity and the County of Los Angeles.

I understand and agree that I may be required to undergo a background and security investigation(s). I understand and agree that my continued performance of work under the above-referenced Master Agreement is contingent upon my passing, to the satisfaction of the County, any and all such investigations. I understand and agree that my failure to pass, to the satisfaction of the County, any such investigation will result in my immediate release from performance under this and/or any future Master Agreement.

CONFIDENTIALITY AGREEMENT:

I may be involved with work pertaining to services provided by the County of Los Angeles and, if so, I may have access to confidential data and information pertaining to persons and/or entities receiving services from the County. In addition, I may also have access to proprietary information supplied by other vendors doing business with the County of Los Angeles. The County has a legal obligation to protect all such confidential data and information in its possession, especially data and information concerning health, criminal, and welfare recipient records. I understand that if I am involved in County work, the County must ensure that I, too, will protect the confidentiality of such data and information. Consequently, I understand that I must sign this agreement as a condition of my work to be provided by the above-referenced Contractor for the County. I have read this agreement and have taken due time to consider it prior to signing.

I hereby agree that I will not divulge to any unauthorized person any data or information obtained while performing work pursuant to the above-referenced Master Agreement between the above-referenced Contractor and the County of Los Angeles. I agree to forward all requests for the release of any data or information received by me to the above-referenced Contractor.

I agree to keep confidential all health, criminal, and welfare recipient records and all data and information pertaining to persons and/or entities receiving services from the County, design concepts, algorithms, programs, formats, documentation, Contractor proprietary information, and all other original materials produced, created, or provided to or by me under the above-referenced Master Agreement. I agree to protect these confidential materials against disclosure to other than the above-referenced Contractor or County employees who have a need to know the information. I agree that if proprietary information supplied by other County vendors is provided to me, I must keep such information confidential.

I agree to report to the above-referenced Contractor any and all violations of this agreement by myself and/or by any other person of whom I become aware. I agree to return all confidential materials to the above-referenced Contractor upon completion of this Master Agreement or termination of my services hereunder, whichever occurs first.

SIGNATURE: _____ DATE: _____

PRINTED NAME: _____

POSITION: _____

CHARITABLE CONTRIBUTIONS CERTIFICATION

Company Name

Address

Internal Revenue Service Employer Identification Number

California Registry of Charitable Trusts "CT" number (if applicable)

The Nonprofit Integrity Act (SB 1262, Chapter 919) added requirements to California's Supervision of Trustees and Fundraisers for Charitable Purposes Act which regulates those receiving and raising charitable contributions.

Check the Certification below that is applicable to your company.

☐ Proposer or Contractor has examined its activities and determined that it does not now receive or raise charitable contributions regulated under California's Supervision of Trustees and Fundraisers for Charitable Purposes Act. If Proposer engages in activities subjecting it to those laws during the term of a County contract, it will timely comply with them and provide County a copy of its initial registration with the California State Attorney General's Registry of Charitable Trusts when filed.

OR

☐ Proposer or Contractor is registered with the California Registry of Charitable Trusts under the CT number listed above and is in compliance with its registration and reporting requirements under California law. Attached is a copy of its most recent filing with the Registry of Charitable Trusts as required by Title 11 California Code of Regulations, sections 300-301 and Government Code sections 12585-12586.

Signature: _____ Date: _____

Printed Name: _____ Title: _____

INFORMATION SECURITY AND PRIVACY REQUIREMENTS EXHIBIT

The County of Los Angeles ("County") is committed to safeguarding the Integrity of the County systems, Data, Information and protecting the privacy rights of the individuals that it serves. This Information Security and Privacy Requirements Exhibit ("Exhibit") sets forth the County and the Contractor's commitment and agreement to fulfill each of their obligations under applicable State or federal laws, rules, or regulations, as well as applicable industry standards concerning privacy, Data protections, Information Security, Confidentiality, Availability, and Integrity of such Information. The Information Security and privacy requirements and procedures in this Exhibit are to be established by the Contractor before the Effective Date of the Contract and maintained throughout the term of the Master Agreement.

These requirements and procedures are a minimum standard and are in addition to the requirements of the underlying base agreement between the County and Contractor (the "Master Agreement") and any other agreements between the parties. However, it is the Contractor's sole obligation to: (i) implement appropriate and reasonable measures to secure and protect its systems and all County Information against internal and external Threats and Risks; and (ii) continuously review and revise those measures to address ongoing Threats and Risks. Failure to comply with the minimum requirements and procedures set forth in this Exhibit will constitute a material, non-curable breach of Master Agreement by the Contractor, entitling the County, in addition to the cumulative of all other remedies available to it at law, in equity, or under the Master Agreement, to immediately terminate the Master Agreement. To the extent there are conflicts between this Exhibit and the Master Agreement, this Exhibit will prevail unless stated otherwise.

1. DEFINITIONS

Unless otherwise defined in the Master Agreement, the definitions herein contained are specific to the uses within this exhibit.

a. **Availability:** the condition of Information being accessible and usable upon demand by an authorized entity (Workforce Member or process).

b. **Confidentiality:** the condition that Information is not disclosed to system entities (users, processes, devices) unless they have been authorized to access the Information.

c. **County Information:** all Data and Information belonging to the County.

d. **Data:** a subset of Information comprised of qualitative or quantitative values.

e. **Incident:** a suspected, attempted, successful, or imminent Threat of unauthorized electronic and/or physical access, use, disclosure, breach, modification, or destruction of information; interference with Information Technology operations; or significant violation of County policy.

f. **Information:** any communication or representation of knowledge or understanding such as facts, Data, or opinions in any medium or form, including electronic, textual, numerical, graphic, cartographic, narrative, or audiovisual.

g. **Information Security Policy:** high level statements of intention and direction of an organization used to create an organization's Information Security Program as formally expressed by its top management.

h. **Information Security Program:** formalized and implemented Information Security Policies, standards and procedures that are documented describing the program management safeguards and common controls in place or those planned for meeting the County's information security requirements.

i. **Information Technology:** any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of Data or Information.

j. **Integrity**: the condition whereby Data or Information has not been improperly modified or destroyed and authenticity of the Data or Information can be ensured.

k. **Mobile Device Management (MDM):** software that allows Information Technology administrators to control, secure, and enforce policies on smartphones, tablets, and other endpoints.

l. **Privacy Policy:** high level statements of intention and direction of an organization used to create an organization's Privacy Program as formally expressed by its top management.

m. **Privacy Program:** A formal document that provides an overview of an organization's privacy program, including a description of the structure of the privacy program, the resources dedicated to the privacy program, the role of the organization's privacy official and other staff, the strategic goals and objectives of the Privacy Program, and the program management controls and common controls in place or planned for meeting applicable privacy requirements and managing privacy risks.

n. **Risk:** a measure of the extent to which the County is threatened by a potential circumstance or event, Risk is typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.

o. **Threat:** any circumstance or event with the potential to adversely impact County operations (including mission, functions, image, or reputation), organizational assets, individuals, or other organizations through an Information System via unauthorized access, destruction, disclosure, modification of Information, and/or denial of service.

p. **Vulnerability:** a weakness in a system, application, network or process that is subject to exploitation or misuse.

q. **Workforce Member:** employees, volunteers, and other persons whose conduct, in the performance of work for Los Angeles County, is under the direct control of Los Angeles County, whether or not they are paid by Los Angeles County. This includes, but may not be limited to, full and part time elected or appointed officials, employees, affiliates, associates, students, volunteers, and staff from third party entities who provide service to the County.

2. INFORMATION SECURITY AND PRIVACY PROGRAMS

a. **Information Security Program.** The Contractor must maintain a company-wide Information Security Program designed to evaluate Risks to the Confidentiality, Availability, and Integrity of the County Information covered under this Master Agreement.

Contractor's Information Security Program must include the creation and maintenance of Information Security Policies, standards, and procedures. Information Security Policies, standards, and procedures will be communicated to all Contractor employees in a relevant, accessible, and understandable form and will be regularly reviewed and evaluated to ensure operational effectiveness, compliance with all applicable laws and regulations, and addresses new and emerging Threats and Risks.

The Contractor must exercise the same degree of care in safeguarding and protecting County Information that the Contractor exercises with respect to its own Information and Data, but in no event less than a reasonable degree of care. The Contractor will implement, maintain, and use appropriate administrative, technical, and physical security measures to preserve the Confidentiality, Integrity, and Availability of County Information.

The Contractor's Information Security Program must:

- Protect the Confidentiality, Integrity, and Availability of County Information in the Contractor's possession or control;
- Protect against any anticipated Threats or hazards to the Confidentiality, Integrity, and Availability of County Information;
- Protect against unauthorized or unlawful access, use, disclosure, alteration, or destruction of County Information;
- Protect against accidental loss or destruction of, or damage to, County Information; and
- Safeguard County Information in compliance with any applicable laws and regulations which apply to the Contractor.

b. **Privacy Program.** The Contractor must establish and maintain a company-wide Privacy Program designed to incorporate Privacy Policies and practices in its business operations to provide safeguards for Information, including County Information. The Contractor's Privacy Program must include the development of, and ongoing reviews and updates to Privacy Policies, guidelines, procedures and appropriate workforce privacy training within its organization. These Privacy Policies, guidelines, procedures, and appropriate training will be provided to all Contractor employees, agents, and volunteers. The Contractor's Privacy Policies, guidelines, and procedures must be continuously reviewed and updated for effectiveness and compliance with applicable laws and regulations, and to appropriately respond to new and emerging Threats and Risks. The Contractor's Privacy Program must perform ongoing monitoring and audits of operations to identify and mitigate privacy Threats.

   The Contractor must exercise the same degree of care in safeguarding the privacy of County Information that the Contractor exercises with respect to its own Information, but in no event less than a reasonable degree of care. The Contractor will implement, maintain, and use appropriate privacy practices and protocols to preserve the Confidentiality of County Information.

   The Contractor's Privacy Program must include:

   - A Privacy Program framework that identifies and ensures that the Contractor complies with all applicable laws and regulations;
   - External Privacy Policies, and internal privacy policies, procedures and controls to support the privacy program;
   - Protections against unauthorized or unlawful access, use, disclosure, alteration, or destruction of County Information;
   - A training program that covers Privacy Policies, protocols and awareness;
   - A response plan to address privacy Incidents and privacy breaches; and
   - Ongoing privacy assessments and audits.

3. PROPERTY RIGHTS TO COUNTY INFORMATION

All County Information is deemed property of the County, and the County will retain exclusive rights and ownership thereto. County Information must not be used by the Contractor for any purpose other than as required under this Master Agreement, nor will such or any part of such be disclosed, sold, assigned, leased, or otherwise disposed of, to third parties by the Contractor, or commercially exploited or otherwise used by, or on behalf of, the Contractor, its officers, directors, employees, or agents. The Contractor may assert no lien on or right to withhold from the County, any County Information it receives from, receives addressed to, or stores on behalf of, the County. Notwithstanding the foregoing, the Contractor may aggregate, compile, and use County Information in order to improve, develop or enhance the System Software and/or other services offered, or to be offered, by the Contractor, provided that (i) no County Information in such aggregated or compiled pool is identifiable as originating from, or can be traced back to the County, and (ii) such Data or Information cannot be associated or matched with the identity of an individual alone, or linkable to a specific individual. The Contractor specifically consents to the County's access to such County Information held, stored, or maintained on any and all devices Contactor owns, leases or possesses.

4. CONTRACTOR'S USE OF COUNTY INFORMATION

The Contractor may use County Information only as necessary to carry out its obligations under this Master Agreement. The Contractor must collect, maintain, or use County Information only for the purposes specified in the Master Agreement and, in all cases, in compliance with all applicable local, State, and federal laws and regulations governing the collection, maintenance, transmission, dissemination, storage, use, and destruction of County Information, including, but not limited to, (i) any State and federal law governing the protection of personal Information, (ii) any State and federal security breach notification laws, and (iii) the rules, regulations and directives of the Federal Trade Commission, as amended from time to time.

5. SHARING COUNTY INFORMATION AND DATA

The Contractor must not share, release, disclose, disseminate, make available, transfer, or otherwise communicate orally, in writing, or by electronic or other means, County Information to a third party for monetary or other valuable consideration.

6. CONFIDENTIALITY

a. **Confidentiality of County Information.** The Contractor agrees that all County Information is Confidential and proprietary to the County regardless of whether such Information was disclosed intentionally or unintentionally, or marked as "confidential".

b. **Disclosure of County Information.** The Contractor may disclose County Information only as necessary to carry out its obligations under this Master Agreement, or as required by law, and is prohibited from using County Information for any other purpose without the prior express written approval of the County's contract administrator in consultation with the County's Chief Information Security Officer and/or Chief Privacy Officer. If required by a court of competent jurisdiction or an administrative body to disclose County Information, the Contractor must notify the County's contract administrator immediately and prior to any such disclosure, to provide the County an opportunity to oppose or otherwise respond to such disclosure, unless prohibited by law from doing so.

c. **Disclosure Restrictions of Non-Public Information.** While performing work under the Master Agreement, the Contractor may encounter County Non-public Information ("NPI") in the course of performing this Master Agreement, including, but not limited to, licensed technology,

drawings, schematics, manuals, sealed court records, and other materials described and/or identified as "Internal Use", "Confidential" or "Restricted" as defined in Board of Supervisors Policy 6.104 – Information Classification Policy as NPI. The Contractor must not disclose or publish any County NPI and material received or used in performance of this Master Agreement. This obligation is perpetual.

d. **Individual Requests.** The Contractor must acknowledge any request or instructions from the County regarding the exercise of any individual's privacy rights provided under applicable federal or State laws. The Contractor must have in place appropriate policies and procedures to promptly respond to such requests and comply with any request or instructions from the County within seven (7) calendar days. If an individual makes a request directly to the Contractor involving County Information, the Contractor must notify the County within five (5) calendar days and the County will coordinate an appropriate response, which may include instructing the Contractor to assist in fulfilling the request. Similarly, if the Contractor receives a privacy or security complaint from an individual regarding County Information, the Contractor must notify the County as described in Section 14 SECURITY AND PRIVACY INCIDENTS, and the County will coordinate an appropriate response.

e. **Retention of County Information.** The Contractor must not retain any County Information for any period longer than necessary for the Contractor to fulfill its obligations under the Master Agreement and applicable law, whichever is longest.

7. CONTRACTOR EMPLOYEES

The Contractor must perform background and security investigation procedures in the manner prescribed in this section unless the Master Agreement prescribes procedures for conducting background and security investigations and those procedures are no less stringent than the procedures described in this section.

To the extent permitted by applicable law, the Contractor must screen and conduct background investigations on all Contractor employees and Subcontractors as appropriate to their role, with access to County Information for potential security Risks. Such background investigations must be obtained through fingerprints submitted to the California Department of Justice to include State, local, and federal-level review and conducted in accordance with the law, may include criminal and financial history to the extent permitted under the law, and will be repeated on a regular basis. The fees associated with the background investigation will be at the expense of the Contractor, regardless of whether the member of the Contractor's staff passes or fails the background investigation. The Contractor, in compliance with its legal obligations, must conduct an individualized assessment of their employees, agents, and volunteers regarding the nature and gravity of a criminal offense or conduct; the time that has passed since a criminal offense or conduct and completion of the sentence; and the nature of the access to County Information to ensure that no individual accesses County Information whose past criminal conduct poses a risk or threat to County Information.

The Contractor must require all employees, agents, and volunteers to abide by the requirements in this Exhibit, as set forth in the Master Agreement, and sign an appropriate written Confidentiality/non-disclosure agreement with the Contractor.

The Contractor must supply each of its employees with appropriate, annual training regarding Information Security procedures, Risks, and Threats. The Contractor agrees that training will cover, but may not be limited to the following topics:

a) **Secure Authentication:** The importance of utilizing secure authentication, including proper management of authentication credentials (login name and password) and multi-factor authentication.

b) **Social Engineering Attacks:** Identifying different forms of social engineering including, but not limited to, phishing, phone scams, and impersonation calls.

c) **Handling of County Information:** The proper identification, storage, transfer, archiving, and destruction of County Information.

d) **Causes of Unintentional Information Exposure:** Provide awareness of causes of unintentional exposure of Information such as lost mobile devices, emailing Information to inappropriate recipients, etc.

e) **Identifying and Reporting Incidents:** Awareness of the most common indicators of an Incident and how such indicators should be reported within the organization.

f) **Privacy:** The Contractor's Privacy Policies and procedures as described in Section 2b. Privacy Program.

The Contractor must have an established set of procedures to ensure the Contractor's employees promptly report actual and/or suspected breaches of security.

8. SUBCONTRACTORS AND THIRD PARTIES

The County acknowledges that in the course of performing its services, the Contractor may desire or require the use of goods, services, and/or assistance of Subcontractors or other third parties or suppliers. The terms of this Exhibit will also apply to all Subcontractors and third parties. The Contractor or third party will be subject to the following terms and conditions: (i) each Subcontractor and third party must agree in writing to comply with and be bound by the applicable terms and conditions of this Exhibit, both for itself and to enable the Contractor to be and remain in compliance with its obligations hereunder, including those provisions relating to Confidentiality, Integrity, Availability, disclosures, security, and such other terms and conditions as may be reasonably necessary to effectuate the Master Agreement including this Exhibit; and (ii) the Contractor will be and remain fully liable for the acts and omissions of each Subcontractor and third party, and fully responsible for the due and proper performance of all Contractor obligations under this Master Agreement.

The Contractor must obtain advanced approval from the County's Chief Information Security Officer and/or Chief Privacy Officer prior to subcontracting services subject to this Exhibit.

9. STORAGE AND TRANSMISSION OF COUNTY INFORMATION

All County Information must be rendered unusable, unreadable, or indecipherable to unauthorized individuals. Without limiting the generality of the foregoing, the Contractor will encrypt all workstations, portable devices (such as mobile, wearables, tablets,) and removable media (such as portable or removable hard disks, floppy disks, USB memory drives, CDs, DVDs, magnetic tape, and all other removable storage media) that store County Information in accordance with Federal Information Processing Standard (FIPS) 140-2 or otherwise approved by the County's Chief Information Security Officer.

The Contractor will encrypt County Information transmitted on networks outside of the Contractor's control with Transport Layer Security (TLS) or Internet Protocol Security **(**IPSec**)**, at a minimum cipher strength of 128 bit or an equivalent secure transmission protocol or method approved by County's Chief Information Security Officer.

In addition, the Contractor must not store County Information in the cloud or in any other online storage provider without written authorization from the County's Chief Information Security Officer. All mobile devices storing County Information must be managed by a Mobile Device Management system. Such system must provide provisions to enforce a password/passcode on enrolled mobile devices. All workstations/Personal Computers (including laptops, 2-in-1s, and tablets) will maintain the latest operating system security patches, and the latest virus definitions. Virus scans must be performed at least monthly. Request for less frequent scanning must be approved in writing by the County's Chief Information Security Officer.

10. RETURN OR DESTRUCTION OF COUNTY INFORMATION

The Contractor must return or destroy County Information in the manner prescribed in this section unless the Master Agreement prescribes procedures for returning or destroying County Information and those procedures are no less stringent than the procedures described in this section.

a. **Return or Destruction.** Upon County's written request, or upon expiration or termination of this Master Agreement for any reason, Contractor must (i) promptly return or destroy, at the County's option, all originals and copies of all documents and materials it has received containing County Information; or (ii) if return or destruction is not permissible under applicable law, continue to protect such Information in accordance with the terms of this Master Agreement; and (iii) deliver or destroy, at the County's option, all originals and copies of all summaries, records, descriptions, modifications, negatives, drawings, adoptions and other documents or materials, whether in writing or in machine-readable form, prepared by the Contractor, prepared under its direction, or at its request, from the documents and materials referred to in Subsection (i) of this Section. For all documents or materials referred to in Subsections (i) and (ii) of this Section that the County requests be returned to the County, the Contractor must provide a written attestation on company letterhead certifying that all documents and materials have been delivered to the County. For documents or materials referred to in Subsections (i) and (ii) of this Section that the County requests be destroyed, the Contractor must provide an attestation on company letterhead and certified documentation from a media destruction firm consistent with subdivision b of this Section. Upon termination or expiration of the Master Agreement or at any time upon the County's request, the Contractor must return all hardware, if any, provided by the County to the Contractor. The hardware should be physically sealed and returned via a bonded courier, or as otherwise directed by the County.

b. **Method of Destruction.** The Contractor must destroy all originals and copies by (i) cross-cut shredding paper, film, or other hard copy media so that the Information cannot be read or otherwise reconstructed; and (ii) purging, or destroying electronic media containing County Information consistent with NIST Special Publication 800-88, "Guidelines for Media Sanitization" such that the County Information cannot be retrieved. The Contractor will provide an attestation on company letterhead and certified documentation from a media destruction firm, detailing the destruction method used and the County Information involved, the date of destruction, and the company or individual who performed the destruction. Such statement will be sent to the designated County contract manager within ten (10) days of termination or expiration of the Master Agreement or at any time upon the County's request. On termination or expiration of this Master Agreement, the County will return or destroy all Contractor's Information marked as confidential (excluding items licensed to the County hereunder, or that provided to the County by the Contractor hereunder), at the County's option.

11. PHYSICAL AND ENVIRONMENTAL SECURITY

All Contractor facilities that process County Information will be located in secure areas and protected by perimeter security such as barrier access controls (e.g., the use of guards and entry badges) that provide a physically secure environment from unauthorized access, damage, and interference.

All Contractor facilities that process County Information will be maintained with physical and environmental controls (temperature and humidity) that meet or exceed hardware manufacturer's specifications.

12. OPERATIONAL MANAGEMENT, BUSINESS CONTINUITY, AND DISASTER RECOVERY

The Contractor must: (i) monitor and manage all of its Information processing facilities, including, without limitation, implementing operational procedures, change management, and Incident response procedures consistent with Section 14 SECURITY AND PRIVACY INCIDENTS; and (ii) deploy adequate anti-malware software and adequate back-up systems to ensure essential business Information can be promptly recovered in the event of a disaster or media failure; and (iii) ensure its operating procedures are adequately documented and designed to protect Information and computer media from theft and unauthorized access.

The Contractor must have business continuity and disaster recovery plans. These plans must include a geographically separate back-up data center and a formal framework by which an unplanned event will be managed to minimize the loss of County Information and services. The formal framework includes a defined back-up policy and associated procedures, including documented policies and procedures designed to: (i) perform back-up of data to a remote back-up data center in a scheduled and timely manner; (ii) provide effective controls to safeguard backed-up data; (iii) securely transfer County Information to and from back-up location; (iv) fully restore applications and operating systems; and (v) demonstrate periodic testing of restoration from back-up location. If the Contractor makes backups to removable media (as described in Section 9 STORAGE AND TRANSMISSION OF COUNTY INFORMATION), all such backups must be encrypted in compliance with the encryption requirements noted above in Section 9 STORAGE AND TRANSMISSION OF COUNTY INFORMATION.

13. ACCESS CONTROL

Subject to and without limiting the requirements under Section 9 STORAGE AND TRANSMISSION OF COUNTY INFORMATION, County Information (i) may only be made available and accessible to those parties explicitly authorized under the Master Agreement or otherwise expressly approved by the County Project Director or Project Manager in writing; and (ii) if transferred using removable media (as described in Section 9 STORAGE AND TRANSMISSION OF COUNTY INFORMATION) must be sent via a bonded courier and protected using encryption technology designated by the Contractor and approved by the County's Chief Information Security Officer in writing. The foregoing requirements will apply to back-up media stored by the Contractor at off-site facilities.

The Contractor must implement formal procedures to control access to County systems, services, and/or Information, including, but not limited to, user account management procedures and the following controls:

a. Network access to both internal and external networked services must be controlled, including, but not limited to, the use of industry standard and properly configured firewalls;

b. Operating systems will be used to enforce access controls to computer resources including, but not limited to, multi-factor authentication, use of virtual private networks (VPN), authorization, and event logging;

c. The Contractor will conduct regular, no less often than semi-annually, user access reviews to ensure that unnecessary and/or unused access to County Information is removed in a timely manner;

d. Applications will include access control to limit user access to County Information and application system functions;

e. All systems will be monitored to detect deviation from access control policies and identify suspicious activity. The Contractor must record, review and act upon all events in accordance with Incident response policies set forth in Section 14 SECURITY AND PRIVACY INCIDENTS; and

f. In the event any hardware, storage media, or removable media (as described in Section 9 STORAGE AND TRANSMISSION OF COUNTY INFORMATION) must be disposed of or sent off-site for servicing, the Contractor must ensure all County Information, has been eradicated from such hardware and/or media using industry best practices as discussed in Section 9 STORAGE AND TRANSMISSION OF COUNTY INFORMATION.

14. SECURITY AND PRIVACY INCIDENTS

In the event of a Security or Privacy Incident, the Contractor must:

a. Promptly notify the County's Chief Information Security Officer, the Departmental Information Security Officer, and the County's Chief Privacy Officer of any Incidents involving County Information, within twenty-four (24) hours of detection of the Incident. All notifications must be submitted via encrypted email and telephone.

County Chief Information Security Officer and Chief Privacy Officer email
CISO-CPO_Notify@lacounty.gov

Chief Information Security Officer:
Jeffrey Aguilar
Chief Information Security Officer
320 W Temple, 7th Floor
Los Angeles, CA 90012
(213) 253-5600

Chief Privacy Officer:
Lillian Russell
Chief Privacy Officer
320 W Temple, 7th Floor
Los Angeles, CA 90012
(213) 351-5363

Departmental Information Security Officer:
Robert Rodgers
Department Information Security Officer II
12851 Crossroads Parkway South
City of Industry, CA 91746
(562) 551-3487
RobertRodgers@dpss.lacounty.gov

b. Include the following Information in all notices:

   i. The date and time of discovery of the Incident,

   ii. The approximate date and time of the Incident,

   iii. A description of the type of County Information involved in the reported Incident, and

   iv. A summary of the relevant facts, including a description of measures being taken to respond to and remediate the Incident, and any planned corrective actions as they are identified.

   v. The name and contact information for the organizations official representative(s), with relevant business and technical information relating to the incident.

c. Cooperate with the County to investigate the Incident and seek to identify the specific County Information involved in the Incident upon the County's written request, without charge, unless the Incident was caused by the acts or omissions of the County. As Information about the Incident is collected or otherwise becomes available to the Contractor, and unless prohibited by law, the Contractor must provide Information regarding the nature and consequences of the Incident that are reasonably requested by the County to allow the County to notify affected individuals, government agencies, and/or credit bureaus.

d. Immediately initiate the appropriate portions of their Business Continuity and/or Disaster Recovery plans in the event of an Incident causing an interference with Information Technology operations.

e. Assist and cooperate with forensic investigators, the County, law firms, and and/or law enforcement agencies at the direction of the County to help determine the nature, extent, and source of any Incident, and reasonably assist and cooperate with the County on any additional disclosures that the County is required to make as a result of the Incident.

f. Allow the County or its third-party designee at the County's election to perform audits and tests of the Contractor's environment that may include, but are not limited to, interviews of relevant employees, review of documentation, or technical inspection of systems, as they relate to the receipt, maintenance, use, retention, and authorized destruction of County Information.

Notwithstanding any other provisions in this Master Agreement and Exhibit, The Contractor will be (i) liable for all damages and fines, (ii) responsible for all corrective action, and (iii) responsible for all notifications arising from an Incident involving County Information caused by the Contractor's weaknesses, negligence, errors, or lack of Information Security or privacy controls or provisions.

15. NON-EXCLUSIVE EQUITABLE REMEDY

The Contractor acknowledges and agrees that due to the unique nature of County Information there can be no adequate remedy at law for any breach of its obligations hereunder, that any such breach may result in irreparable harm to the County, and therefore, that upon any such breach, the County will be entitled to appropriate equitable remedies, and may seek injunctive relief from a court of competent jurisdiction without the necessity of proving actual loss, in addition to whatever remedies are available within law or equity. Any breach of Section 6 CONFIDENTIALITY will constitute a material breach of this Master Agreement and be grounds for immediate termination of this Master Agreement in the exclusive discretion of the County.

16. AUDIT AND INSPECTION

a. **Self-Audits.** The Contractor must periodically conduct audits, assessments, testing of the system of controls, and testing of Information Security and privacy procedures, including

penetration testing, intrusion detection, and firewall configuration reviews. These periodic audits will be conducted by staff certified to perform the specific audit in question at Contractor's sole cost and expense through either (i) an internal independent audit function, (ii) a nationally recognized, external, independent auditor, or (iii) another independent auditor approved by the County.

The Contractor must have a process for correcting control deficiencies that have been identified in the periodic audit, including follow up documentation providing evidence of such corrections. The Contractor must provide the audit results and any corrective action documentation to the County promptly upon its completion at the County's request. With respect to any other report, certification, or audit or test results prepared or received by the Contractor that contains any County Information, the Contractor must promptly provide the County with copies of the same upon the County's reasonable request, including identification of any failure or exception in the Contractor's Information systems, products, and services, and the corresponding steps taken by the Contractor to mitigate such failure or exception. Any reports and related materials provided to the County pursuant to this Section must be provided at no additional charge to the County.

b. **County Requested Audits.** At its own expense, the County, or an independent third-party auditor commissioned by the County, will have the right to audit the Contractor's infrastructure, security and privacy practices, Data center, services and/or systems storing or processing County Information via an onsite inspection at least once a year. Upon the County's request the Contractor must complete a questionnaire regarding Contractor's Information Security and/or program. The County will pay for the County requested audit unless the auditor finds that the Contractor has materially breached this Exhibit, in which case the Contractor must bear all costs of the audit**;** and if the audit reveals material non-compliance with this Exhibit, the County may exercise its termination rights underneath the Master Agreement.

   Such audit will be conducted during the Contractor's normal business hours with reasonable advance notice, in a manner that does not materially disrupt or otherwise unreasonably and adversely affect the Contractor's normal business operations. The County's request for the audit will specify the scope and areas (e.g., Administrative, Physical, and Technical) that are subject to the audit and may include, but are not limited to physical controls inspection, process reviews, policy reviews, evidence of external and internal Vulnerability scans, penetration test results, evidence of code reviews, and evidence of system configuration and audit log reviews. It is understood that the results may be filtered to remove the specific Information of other Contractor customers such as IP address, server names, etc. The Contractor must cooperate with the County in the development of the scope and methodology for the audit, and the timing and implementation of the audit. This right of access will extend to any regulators with oversight of the County. The Contractor agrees to comply with all reasonable recommendations that result from such inspections, tests, and audits within reasonable timeframes.

   When not prohibited by regulation, the Contractor will provide to the County a summary of: (i) the results of any security audits, security reviews, or other relevant audits, conducted by the Contractor or a third party; and (ii) corrective actions or modifications, if any, the Contractor will implement in response to such audits.

17. CYBER LIABILITY INSURANCE

The Contractor must secure and maintain cyber liability insurance coverage in the manner prescribed in this section unless the Master Agreement prescribes cyber liability insurance coverage provisions and those provisions are no less stringent than those described in this section.

The Contractor must secure and maintain cyber liability insurance coverage with limits of at least **$2,000,000** per occurrence and in the aggregate during the term of the Master Agreement, including coverage for: network security liability; privacy liability; privacy regulatory proceeding defense, response, expenses and fines; technology professional liability (errors and omissions); privacy breach expense reimbursement (liability arising from the loss or disclosure of County Information no matter how it occurs); system breach; denial or loss of service; introduction, implantation, or spread of malicious software code; unauthorized access to or use of computer systems; and Data/Information loss and business interruption; any other liability or risk that arises out of the Master Agreement. The Contractor must add the County as an additional insured to its cyber liability insurance policy and provide to the County certificates of insurance evidencing the foregoing upon the County's request. The procuring of the insurance described herein, or delivery of the certificates of insurance described herein, must not be construed as a limitation upon the Contractor's liability or as full performance of its indemnification obligations hereunder. No exclusion/restriction for unencrypted portable devices/media may be on the policy.

18. PRIVACY AND SECURITY INDEMNIFICATION

In addition to the indemnification provisions in the Master Agreement, the Contractor agrees to indemnify, defend, and hold harmless the County, its Special Districts, elected and appointed officers, agents, employees, and volunteers from and against any and all claims, demands liabilities, damages, judgments, awards, losses, costs, expenses or fees including reasonable attorneys' fees, accounting and other expert, consulting or professional fees, and amounts paid in any settlement arising from, connected with, or relating to:

- The Contractor's violation of any federal and State laws in connection with its accessing, collecting, processing, storing, disclosing, or otherwise using County Information;
- The Contractor's failure to perform or comply with any terms and conditions of this Master Agreement or related agreements with the County; and/or,
- Any Information loss, breach of Confidentiality, or Incident involving any County Information that occurs on the Contractor's systems or networks (including all costs and expenses incurred by the County to remedy the effects of such loss, breach of Confidentiality, or Incident, which may include (i) providing appropriate notice to individuals and governmental authorities, (ii) responding to individuals' and governmental authorities' inquiries, (iii) providing credit monitoring to individuals, and (iv) conducting litigation and settlements with individuals and governmental authorities).

Notwithstanding the preceding sentences, the County will have the right to participate in any such defense at its sole cost and expense, except that in the event contractor fails to provide County with a full and adequate defense, as determined by County in its sole judgment, County will be entitled to retain its own counsel, including, without limitation, County Counsel, and to reimbursement from contractor for all such costs and expenses incurred by County in doing so. Contractor will not have the right to enter into any settlement, agree to any injunction or other equitable relief, or make any admission, in each case, on behalf of County without County's prior written approval.

ADDENDUM A: SOFTWARE AS A SERVICE (SaaS)

a. **License:** Subject to the terms and conditions set forth in this Master Agreement, including payment of the license fees by to the Contractor, the Contractor hereby grants to County a non-exclusive, non-transferable worldwide County license to use the SaaS, as well as any documentation and training materials, during the term of this Master Agreement to enable the County to use the full benefits of the SaaS and achieve the purposes stated herein.

b. **Business Continuity:** In the event that the Contractor's infrastructure containing or processing County Information becomes lost, altered, damaged, interrupted, destroyed, or otherwise limited in functionality in a way that affects the County's use of the SaaS, The Contractor must immediately and within twenty-four (24) hours implement the Contractor's Business Continuity Plan, consistent with Section 12 OPERATIONAL MANAGEMENT, BUSINESS CONTINUITY, AND DISASTER RECOVERY, such that the Contractor can continue to provide full functionality of the SaaS as described in the Master Agreement.

   The Contractor will indemnify the County for any claims, losses, or damages arising out of the County's inability to use the SaaS consistent with the Master Agreement and Section 0 18. PRIVACY AND SECURITY INDEMNIFICATION.

   The Contractor must include in its Business Continuity Plan service offering, a means for segmenting and distributing IT infrastructure, disaster recovery and mirrored critical system, among any other measures reasonably necessary to ensure business continuity and provision of the SaaS.

   In the event that the SaaS is interrupted, the County Information may be accessed and retrieved within two (2) hours at any point in time. To the extent the Contractor hosts County Information related to the SaaS, the Contractor must create daily backups of all County Information related to the County's use of the SaaS in a segmented or off-site "hardened" environment in a manner that ensures backups are secure consistent with cybersecurity requirements described in this Master Agreement and available when needed.

c. **Enhancements:** Upgrades, replacements and new versions: The Contractor agrees to provide to County, at no cost, prior to, and during installation and implementation of the SaaS any software/firmware enhancements, upgrades, and replacements which the Contractor initiates or generates that are within the scope of the SaaS and that are made available at no charge to the Contractor's other customers.

   During the term of this Master Agreement, the Contractor must promptly notify the County of any available updates, enhancements or newer versions of the SaaS and within thirty (30) Days update or provide the new version to the County. The Contractor must provide any accompanying documentation in the form of new or revised documentation necessary to enable the County to understand and use the enhanced, updated, or replaced SaaS.

   During the Master Agreement term, the Contractor must not delete or disable a feature or functionality of the SaaS unless the Contractor provides sixty (60) Days advance notice and the County provides written consent to delete or disable the feature or functionality. Should there be a replacement feature or functionality, the County will have the sole discretion whether to accept such replacement. The replacement will be at no additional cost to the County. If the Contractor fails to abide by the obligations in this section, the County reserves the right to terminate the Master Agreement for material breach and receive a pro-rated refund.

d. **Location of County Information:** The Contractor warrants and represents that it will store and process County Information only in the continental United States and that at no time will County Data traverse the borders of the continental United States in an unencrypted manner.

e. **Audit and Certification:** The Contractor agrees to conduct an annual System and Organization Controls (SOC 2 type II) audit or equivalent (i.e. The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) 27001:2013 certification audit or Health Information Trust Alliance (HITRUST) Common Security Framework certification audit) of its internal controls for security, availability, integrity, confidentiality, and privacy. The Contractor must have a process for correcting control deficiencies that have been identified in the audit, including follow up documentation providing evidence of such corrections. The results of the audit and the Contractor's plan for addressing or resolving the audit findings must be shared with County's Chief Information Security Officer within ten (10) business days of the Contractor's receipt of the audit results. The Contractor agrees to provide County with the current audit certifications upon request.

f. **Services Provided by a Subcontractor:** Prior to the use of any Subcontractor for the SaaS under this Master Agreement, the Contractor must notify County of the proposed subcontractor(s) and the purposes for which they may be engaged at least thirty (30) Days prior to engaging the Subcontractor and obtain written consent of the County's Contract Administrator.

g. **Information Import Requirements at Termination:** Within one (1) Day of notification of termination of this Master Agreement, the Contractor must provide County with a complete, portable, and secure copy of all County Information, including all schema and transformation definitions and/or delimited text files with documented, detailed schema definitions along with attachments in a format to be determined by County upon termination.

h. **Termination Assistance Services:** During the ninety (90) Day period prior to, and/or following the expiration or termination of this Master Agreement, in whole or in part, the Contractor agrees to provide reasonable termination assistance services at no additional cost to County, which may include:

    i. Developing a plan for the orderly transition of the terminated or expired SaaS from the Contractor to a successor;

    ii. Providing reasonable training to County staff or a successor in the performance of the SaaS being performed by the Contractor;

    iii. Using its best efforts to assist and make available to the County any third-party services then being used by the Contractor in connection with the SaaS; and

    iv. Such other activities upon which the Parties may reasonably agree.

ADDENDUM B: CONTRACTOR HARDWARE CONNECTING TO COUNTY SYSTEMS

Notwithstanding any other provisions in this Master Agreement, the Contractor must ensure the following provisions and security controls are established for any and all Systems or Hardware provided under this Master Agreement.

a. **Inventory:** The Contractor must actively manage, including through inventory, tracking, loss prevention, replacement, updating, and correcting, all hardware devices covered under this Master Agreement. The Contractor must be able to provide such management records to the County at inception of the Master Agreement and upon request.

b. **Access Control:** The Contractor agrees to manage access to all Systems or Hardware covered under this Master Agreement. This includes industry-standard management of administrative privileges including, but not limited to, maintaining an inventory of administrative privileges, changing default passwords, use of unique passwords for each individual accessing Systems or Hardware under this Master Agreement, and minimizing the number of individuals with administrative privileges to those strictly necessary. Prior to effective date of this Master Agreement, the Contractor must document their access control plan for Systems or Hardware covered under this Master Agreement and provide such plan to the Department Information Security Officer (DISO) who will consult with the County's Chief Information Security Officer (CISO) for review and approval. The Contractor must modify and/or implement such plan as directed by the DISO and CISO.

c. **Operating System and Equipment Hygiene:** The Contractor agrees to ensure that Systems or Hardware will be kept up to date, using only the most recent and supported operating systems, applications, and programs, including any patching or other solutions for vulnerabilities, within ninety (90) Days of the release of such updates, upgrades, or patches. The Contractor agrees to ensure that the operating system is configured to eliminate any unnecessary applications, services and programs. If for some reason the Contractor cannot do so within ninety (90) Days, the Contractor must provide a Risk assessment to the County's Chief Information Security Officer (CISO).

d. **Vulnerability Management:** The Contractor agrees to continuously acquire, assess, and take action to identify and remediate vulnerabilities within the Systems and Hardware covered under this Master Agreement. If such vulnerabilities cannot be addressed, The Contractor must provide a Risk assessment to the Department Information Security Officer (DISO) who will consult with the County's Chief Information Security Officer (CISO). The County's CISO must approve the Risk acceptance and the Contractor accepts liability for Risks that result to the County for exploitation of any un-remediated vulnerabilities.

e. **Media Encryption:** Throughout the duration of this Master Agreement, the Contractor will encrypt all workstations, portable devices (e.g., mobile, wearables, tablets,) and removable media (e.g., portable or removable hard disks, floppy disks, USB memory drives, CDs, DVDs, magnetic tape, and all other removable storage media) associated with Systems and Hardware provided under this Master Agreement in accordance with Federal Information Processing Standard (FIPS) 140-2 or otherwise required or approved by the County's Chief Information Security Officer (CISO).

f. **Malware Protection:** The Contractor will provide and maintain industry-standard endpoint antivirus and antimalware protection on all Systems and Hardware as approved or required by the Department Information Security Officer (DISO) who will consult with the County's Chief Information Security Officer (CISO) to ensure provided hardware is free, and remains free of malware. The Contractor agrees to provide the County documentation proving malware protection status upon request.

ADDENDUM C: APPLICATION SOURCE CODE REPOSITORY

The Contractor must manage the source code in the manner prescribed in this Addendum unless the Master Agreement prescribes procedures for managing the source code and those procedures are no less stringent than the procedures described in this addendum.

a. **County Application Source Code**. To facilitate the centralized management, reporting, collaboration, and continuity of access to the most current production version of application source code, all code, artifacts, and deliverables produced under this Master Agreement, (hereinafter referred to as "County Source Code") must be version controlled, stored, and delivered on a single industry-standard private Git repository, provided, managed, and supported by the County. Upon commencement of the Master Agreement period, the Contractor will be granted access to the County's private Git repository.

b. **Git Repository.** The Contractor will use the County Git repository during the entire lifecycle of the project from inception to final delivery. The Contractor will create and document design documents, Data flow diagrams, security diagrams, configuration settings, software or hardware requirements and specifications, attribution to third-party code, libraries and all dependencies, and any other documentation related to all County Source Code and corresponding version-controlled documentation within the Git repository. This documentation must include an Installation Guide and a User Guide for the final delivered source code such that County may download, install, and make full functional use of the delivered code as specified and intended.

CDSS
PAT LEARY
ACTING DIRECTOR

STATE OF CALIFORNIA—HEALTH AND HUMAN SERVICES AGENCY
DEPARTMENT OF SOCIAL SERVICES
744 P Street • Sacramento, CA 95814 • *www.cdss.ca.gov*

GAVIN NEWSOM
GOVERNOR

June 25, 2019

ERRATA

ALL COUNTY LETTER (ACL) NO. 19-56E

TO: ALL COUNTY WELFARE DIRECTORS

SUBJECT: **ERRATUM TO ACL 19-56 - 2019 CDSS PRIVACY AND SECURITY AGREEMENT (PSA)**

The purpose of this errata is to transmit an updated copy of the Privacy and Security Agreement (PSA) form. Please ensure to use this attached form in place of the original form transmitted with ACL 19-56.

If there are any questions or concerns regarding the updated Agreement, please contact the Information Security & Privacy Bureau's PSA email box at cdsspsa@dss.ca.gov.

Sincerely,

Original Document Signed By:

NOLA NIEGEL, Branch Chief
Project Oversight and Strategic Technology Branch
Information Systems Division

Attachment

2019 PRIVACY AND SECURITY AGREEMENT

BETWEEN

the California Department of Social Services and the

County of _____,

Department/Agency of _____

PREAMBLE

The California Department of Social Services (CDSS) and the

County of _____,

Department/Agency of _____

enter into this Data Privacy and Security Agreement (Agreement) in order to ensure the privacy and security of Social Security Administration (SSA), Medi-Cal Eligibility Data System (MEDS) and Applicant Income and Eligibility Verification System (IEVS) Personally Identifiable Information (PII), covered by this Agreement and referred to hereinafter as PII, that the counties access through CDSS and the Department of Health Care Services (DHCS). This Agreement covers the following programs:

- CalFresh;
- California Food Assistance Program (CFAP);
- California Work Opportunity and Responsibility to Kids Program (CalWORKs);
- Cash Assistance Program for Immigrants (CAPI);
- Entrant Cash Assistance (ECA)/Refugee Cash Assistance (RCA);
- Foster Care (FC) (eligibility);
- Kinship Guardianship Assistance Program (Kin-GAP) (eligibility);
- Federal Guardianship Assistance Program (Fed-GAP) (eligibility);
- General Assistance/General Relief (GA/GR); and
- Trafficking and Crime Victims Assistance Program (TCVAP).

The CDSS has an Inter-Agency Agreement (IAA) with DHCS that allows CDSS and local county agencies to access SSA and MEDS data in order to Assist in the Administration of the Program for the programs listed above. The IAA requires that CDSS may only share SSA and MEDS data if its contract with the entity with whom it intends to share the data reflects the entity's obligations under the IAA.

The County Department/Agency utilizes SSA and MEDS data in conjunction with other system data in order to Assist in the Administration of the Program for the programs listed above.

This Agreement covers the

County of _____,

Department/Agency of _____

and its staff (County Workers), who access, use, or disclose PII covered by this Agreement, to assist in the administration of programs.

DEFINITIONS

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

1. "**Assist in the Administration of the Program**" means performing administrative functions on behalf of programs, such as determining eligibility for, or enrollment in, and collecting PII for such purposes, to the extent such activities are authorized by law.
2. "**Breach**" refers to actual loss, loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for other than authorized purposes have access or potential access to PII, whether electronic, paper, verbal, or recorded.
3. "**County Worker**" means those county employees, contractors, subcontractors, vendors and agents performing any functions for the county that require access to and/or use of PII and that are authorized by the county to access and use PII.
4. "**PII**" is personally identifiable information directly obtained in the course of performing an administrative function through the MEDS or IEVS systems on behalf of the programs, which can be used alone, or in conjunction with any other reasonably available information to identify a specific individual. PII includes any information that can be used to search for or identify individuals, or can be used to access their files, including, but not limited to name, social security number (SSN), date and place of birth (DOB), mother's maiden name, driver's license number, or identification number. PII may also include any information that is linkable to an individual, such as medical, educational, financial, and employment information. PII may be electronic, paper, verbal, or recorded and includes statements made by, or attributed to, the individual.

5. "**Security Incident**" means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of PII, or interference with system operations in an information system which processes PII that is under the control of the county or county's Statewide Automated Welfare System (SAWS) Consortium, or under the control of a contractor, subcontractor or vendor of the county, on behalf of the county.
6. "**Secure Areas**" means any area where:
   a. County Workers assist in the administration of their program;
   b. County Workers use or disclose PII; or
   c. PII is stored in paper or electronic format.
7. "**SSA-provided or verified data (SSA data)**" means:
   a. Any information under the control of the Social Security Administration (SSA) provided to CDSS under the terms of an information exchange agreement with SSA (e.g., SSA provided date of death, SSA Title II or Title XVI benefit and eligibility data, or SSA citizenship verification); or;
   b. Any information provided to CDSS, including a source other than SSA, but in which CDSS attests that SSA verified it, or couples the information with data from SSA to certify the accuracy of it (e.g. SSN and associated SSA verification indicator displayed together on a screen, file, or report, or DOB and associated SSA verification indicator displayed together on a screen, file, or report).

   For a more detailed definition of "SSA data", please refer to Section 7 of the "Electronic Information Exchange Security Requirements and Procedures for State and Local Agencies Exchanging Electronic Information with SSA" document, an attachment of Exhibit A.

AGREEMENTS

CDSS and County Department/Agency mutually agree as follows:

I. PRIVACY AND CONFIDENTIALITY

A. County Workers may use or disclose PII only as permitted in this Agreement and only to assist in the administration of programs in accordance with 45 CFR § 205.50 et seq. and Welfare and Institutions Code section 10850 or as authorized or required by law. Disclosures required by law or that are made with the explicit written authorization of the client are allowable. Any other use or disclosure of PII requires the express approval in writing of CDSS. No County Worker shall duplicate, disseminate or disclose PII except as allowed in this Agreement.

B. Pursuant to this Agreement, County Workers may only use PII to assist in administering their respective programs.

C. Access to PII shall be restricted to County Workers who need to perform their official duties to assist in the administration of their respective programs.

D. County Workers who access, disclose or use PII in a manner or for a purpose not authorized by this Agreement may be subject to civil and criminal sanctions contained in applicable federal and state statutes.

II. PERSONNEL CONTROLS

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

A. ***Employee Training***. Train and use reasonable measures to ensure compliance with the requirements of this Agreement by County Workers, including, but not limited to:

1. Provide initial privacy and security awareness training to each new County Worker within thirty (30) days of employment;

2. Thereafter, provide annual refresher training or reminders of the privacy and security safeguards in this Agreement to all County Workers. Three (3) or more security reminders per year are recommended;

3. Maintain records indicating each County Worker's name and the date on which the privacy and security awareness training was completed; and
4. Retain training records for a period of three (3) years after completion of the training.

B. ***Employee Discipline***.

1. Provide documented sanction policies and procedures for County Workers who fail to comply with privacy policies and procedures or any provisions of these requirements.
2. Sanction policies and procedures shall include termination of employment when appropriate.

C. ***Confidentiality Statement***. Ensure that all County Workers sign a confidentiality statement. The statement shall be signed by County Workers prior to accessing PII and annually thereafter. Signatures may be physical or electronic. The signed statement shall be retained for a period of three (3) years, or five (5) years if the signed statement is being used to comply with Section 5.10 of the SSA's "Electronic Information Exchange Security Requirements and Procedures for State and Local Agencies Exchanging Electronic Information with SSA" document, an attachment of Exhibit A.

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

1. General Use of the PII;
2. Security and Privacy Safeguards for the PII;
3. Unacceptable Use of the PII; and
4. Enforcement Policies.

D. ***Background Screening***.

1. Conduct a background screening of a County Worker before they may access PII.
2. The background screening should be commensurate with the risk and magnitude of harm the employee could cause. More thorough screening shall be done for those employees who are authorized to bypass significant technical and operational security controls.

3. The County Department/Agency shall retain each County Worker's background screening documentation for a period of three (3) years following conclusion of employment relationship.

III. MANAGEMENT OVERSIGHT AND MONITORING

To ensure compliance with the privacy and security safeguards in this Agreement the County Department/Agency shall perform the following:

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

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

IV. INFORMATION SECURITY AND PRIVACY STAFFING

The County Department/Agency agrees to:

A. Designate information security and privacy officials who are accountable for compliance with these and all other applicable requirements stated in this Agreement.

B. Provide CDSS with applicable contact information for these designated individuals by emailing CDSS at cdsspsa@dss.ca.gov. Any changes to this information should be reported to CDSS within ten (10) days.

C. Assign County Workers to be responsible for administration and monitoring of all security related controls stated in this Agreement.

V. PHYSICAL SECURITY

The County Department/Agency shall ensure PII is used and stored in an area that is physically safe from access by unauthorized persons at all times. The County Department/Agency agrees to safeguard PII from loss, theft, or inadvertent disclosure and, therefore, agrees to:

A. Secure all areas of the County Department/Agency facilities where County Workers assist in the administration of their program and use, disclose, or store PII.

B. These areas shall be restricted to only allow access to authorized individuals by using one or more of the following:

1. Properly coded key cards
2. Authorized door keys
3. Official identification

C. Issue identification badges to County Workers.

D. Require County Workers to wear these badges where PII is used, disclosed, or stored.

E. Ensure each physical location, where PII is used, disclosed, or stored, has procedures and controls that ensure an individual who is terminated from access to the facility is promptly escorted from the facility by an authorized employee and access is revoked.

F. Ensure there are security guards or a monitored alarm system at all times at the County Department/Agency facilities and leased facilities where five hundred (500) or more individually identifiable records of PII is used, disclosed, or stored. Video surveillance systems are recommended.

G. Ensure data centers with servers, data storage devices, and/or critical network infrastructure involved in the use, storage, and/or processing of PII have perimeter security and physical access controls that limit access to only authorized County Workers. Visitors to the data center area shall be escorted at all times by authorized County Workers.

H. Store paper records with PII in locked spaces, such as locked file cabinets, locked file rooms, locked desks, or locked offices in facilities which are multi-use meaning that there are County Department/Agency and non-County Department/Agency functions in one building in work areas that are not securely segregated from each other. It is recommended that all PII be locked up when unattended at any time, not just within multi-use facilities.

I. The County Department/Agency shall have policies based on applicable factors that include, at a minimum, a description of the circumstances under which the County Workers can transport PII, as well as the physical security requirements during transport. A County Department/Agency that chooses to permit its County Workers to leave records unattended in vehicles shall include provisions in its policies to ensure that the PII is stored in a non-visible area such as a trunk, that the vehicle is locked, and that under no circumstances permit PII be left unattended in a vehicle overnight or for other extended periods of time.

J. The County Department/Agency shall have policies that indicate County Workers are not to leave records with PII unattended at any time in airplanes, buses, trains, etc., inclusive of baggage areas. This should be included in training due to the nature of the risk.

K. Use all reasonable measures to prevent non-authorized personnel and visitors from having access to, control of, or viewing PII.

VI. TECHNICAL SECURITY CONTROLS

A. ***Workstation/Laptop Encryption***. All workstations and laptops, which use, store and/or process PII, shall be encrypted using a FIPS 140-2 certified algorithm 128 bit or higher, such as Advanced Encryption Standard (AES). The encryption solution shall be full disk. It is encouraged, when available and when feasible, that the encryption be 256 bit.

B. ***Server Security***. Servers containing unencrypted PII shall have sufficient administrative, physical, and technical controls in place to protect that data, based upon a risk assessment/system security review. It is recommended to follow the guidelines documented in the latest revision of the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Security and Privacy Controls for Federal Information Systems and Organizations.

C. ***Minimum Necessary***. Only the minimum necessary amount of PII required to perform required business functions may be accessed, copied, downloaded, or exported.

D. ***Mobile Device and Removable Media***. All electronic files, which contain PII, shall be encrypted when stored on any mobile device or removable media (i.e. USB drives, CD/DVD, smartphones, tablets, backup tapes etc.). Encryption shall be a FIPS 140-2 certified algorithm 128 bit or higher, such as AES. It is encouraged, when available and when feasible, that the encryption be 256 bit.

E. ***Antivirus Software***. All workstations, laptops and other systems, which process and/or store PII, shall install and actively use an antivirus software solution. Antivirus software should have automatic updates for definitions scheduled at least daily.

F. ***Patch Management***.

1. All workstations, laptops and other systems, which process and/or store PII, shall have critical security patches applied, with system reboot if necessary.

2. There shall be a documented patch management process that determines installation timeframe based on risk assessment and vendor recommendations.
3. At a maximum, all applicable patches deemed as critical shall be installed within thirty (30) days of vendor release. It is recommended that critical patches which are high risk be installed within seven (7) days.
4. Applications and systems that cannot be patched within this time frame, due to significant operational reasons, shall have compensatory controls implemented to minimize risk.

G. ***User IDs and Password Controls***.

1. All users shall be issued a unique user name for accessing PII.
2. Username shall be promptly disabled, deleted, or the password changed within, at most, twenty-four (24) hours of the transfer or termination of an employee. Note: Twenty-four (24) hours is defined as one (1) working day.
3. Passwords are not to be shared.
4. Passwords shall be at least eight (8) characters.
5. Passwords shall be a non-dictionary word.
6. Passwords shall not be stored in readable format on the computer or server.
7. Passwords shall be changed every ninety (90) days or less. It is recommended that passwords be required to be changed every sixty (60) days or less. Non-expiring passwords are permitted when in full compliance with NIST SP 800-63B Authenticator Assurance Level (AAL) 2.
8. Passwords shall be changed if revealed or compromised.

9. Passwords shall be composed of characters from at least three (3) of the four (4) of the following groups from the standard keyboard:
    a. Upper case letters (A-Z)
    b. Lower case letters (a-z)
    c. Arabic numerals (0-9)
    d. Special characters (!,@,#, etc.)

H. ***User Access***. In conjunction with CDSS and DHCS, County Department/Agency management should exercise control and oversight over the authorization of individual user access to SSA data via, MEDS, IEVS, and over the process of issuing and maintaining access control numbers, IDs, and passwords.

I. ***Data Destruction***. When no longer needed, all PII shall be cleared, purged, or destroyed consistent with NIST SP 800-88, Guidelines for Media Sanitization, such that the PII cannot be retrieved.

J. ***System Timeout***. The systems providing access to PII shall provide an automatic timeout, requiring re-authentication of the user session after no more than twenty (20) minutes of inactivity.

K. ***Warning Banners***. The systems providing access to PII shall display a warning banner stating, at a minimum:
    1. Data is confidential;
    2. Systems are logged;
    3. System use is for business purposes only, by authorized users; and
    4. Users shall log off the system immediately if they do not agree with these requirements.

L. ***System Logging***.
    1. The systems that provide access to PII shall maintain an automated audit trail that can identify the user or system process which initiates a request for PII, or alters PII.

2. The audit trail shall:
    a. Be date and time stamped;
    b. Log both successful and failed accesses;
    c. Be read-access only; and
    d. Be restricted to authorized users of the audit trail.
3. If PII is stored in a database, database logging functionality shall be enabled.
4. Audit trail data shall be archived for at least three (3) years from the occurrence.

M. ***Access Controls***. The system providing access to PII shall use role-based access controls for all user authentications, enforcing the principle of least privilege.

N. ***Transmission Encryption***.

1. All data transmissions of PII outside of a secure internal network shall be encrypted using a Federal Information Processing Standard (FIPS) 140-2 certified algorithm that is 128 bit or higher, such as Advanced Encryption Standard (AES) or Transport Layer Security (TLS). It is encouraged, when available and when feasible, that 256-bit encryption be used.
2. Encryption can be end to end at the network level, or the data files containing PII can be encrypted.
3. This requirement pertains to any type of PII in motion such as website access, file transfer, and email.

O. ***Intrusion Prevention***. All systems involved in accessing, storing, transporting, and protecting PII, which are accessible through the Internet, shall be protected by an intrusion detection and prevention solution.

VII. AUDIT CONTROLS

A. ***System Security Review***.

1. The County Department/Agency shall ensure audit control mechanisms are in place.

2. All systems processing and/or storing PII shall have at least an annual system risk assessment/security review that ensures administrative, physical, and technical controls are functioning effectively and provide an adequate level of protection.

3. Reviews should include vulnerability scanning tools.

B. ***Log Reviews***. All systems processing and/or storing PII shall have a process or automated procedure in place to review system logs for unauthorized access.

C. ***Change Control***. All systems processing and/or storing PII shall have a documented change control process that ensures separation of duties and protects the confidentiality, integrity and availability of data.

D. ***Anomalies***. When the County Department/Agency or DHCS suspects MEDS usage anomalies, the County Department/Agency will work with DHCS to investigate the anomalies and report conclusions of such investigations and remediation to CDSS.

VIII. BUSINESS CONTINUITY / DISASTER RECOVERY CONTROLS

A. ***Emergency Mode Operation Plan***. The County Department/Agency shall establish a documented plan to enable continuation of critical business processes and protection of the security of PII kept in an electronic format in the event of an emergency. Emergency means any circumstance or situation that causes normal computer operations to become unavailable for use in performing the work required under this Agreement for more than twenty-four (24) hours. It is recommended that County Department/Agency conduct periodic disaster recovery testing, including connectivity exercises conducted with DHCS and CDSS, if requested.

B. ***Data Centers***. Data centers with servers, data storage devices, and critical network infrastructure involved in the use, storage and/or processing of PII, shall include environmental protection such as cooling, power, and fire prevention, detection, and suppression; and appropriate protection from other threats, including but not limited to flood, earthquake, and terrorism.

C. ***Data Backup and Recovery Plan***.

1. The County Department/Agency shall have established documented procedures to backup PII to maintain retrievable exact copies of PII.

2. The documented backup procedures shall contain a schedule which includes incremental and full backups.

3. The procedures shall include storing backups containing PII offsite.
4. The procedures shall ensure an inventory of backup media.
5. The County Department/Agency shall have established documented procedures to recover PII data.
6. The documented recovery procedures shall include an estimate of the amount of time needed to restore the PII data.
7. It is recommended that the County Department/Agency periodically test the data recovery process.

IX. PAPER DOCUMENT CONTROLS

A. ***Supervision of Data***. The PII in paper form shall not be left unattended at any time, unless it is locked in a file cabinet, file room, desk or office. Unattended means that information may be observed by an individual not authorized to access the information.

B. ***Data in Vehicles***. The County Department/Agency shall have policies that include, based on applicable risk factors, a description of the circumstances under which the County Workers can transport PII, as well as the physical security requirements during transport. A County Department/Agency that chooses to permit its County Workers to leave records unattended in vehicles, it shall include provisions in its policies to provide that the PII is stored in a non-visible area such as a trunk, that the vehicle is locked, and that under no circumstances permit PII to be left unattended in a vehicle overnight or for other extended periods of time.

C. ***Public Modes of Transportation***. The PII in paper form shall not be left unattended at any time in airplanes, buses, trains, etc., inclusive of baggage areas. This should be included in training due to the nature of the risk.

D. ***Escorting Visitors***. Visitors to areas where PII is contained shall be escorted, and PII shall be kept out of sight while visitors are in the area.

E. ***Confidential Destruction***. PII shall be disposed of through confidential means, such as cross cut shredding or pulverizing.

F. ***Removal of Data***. The PII shall not be removed from the premises of County Department/Agency except for identified routine business purposes or with express written permission of CDSS.

G. ***Faxing***.

1. Faxes containing PII shall not be left unattended and fax machines shall be in secure areas.
2. Faxes shall contain a confidentiality statement notifying persons receiving faxes in error to destroy them and notify the sender.
3. Fax numbers shall be verified with the intended recipient before sending the fax.

H. ***Mailing***.

1. Mailings containing PII shall be sealed and secured from damage or inappropriate viewing of PII to the extent possible.
2. Mailings that include five hundred (500) or more individually identifiable records containing PII in a single package shall be sent using a tracked mailing method that includes verification of delivery and receipt, unless the County Department/Agency obtains prior written permission from CDSS to use another method.

X. NOTIFICATION AND INVESTIGATION OF BREACHES AND SECURITY INCIDENTS

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

A. ***Initial Notice to DHCS***:

The County Department/Agency will provide initial notice to DHCS by email, or alternatively, by telephone if email is unavailable, of any suspected security incident, intrusion, or unauthorized access, use, or disclosure of PII or potential loss of PII with a copy to CDSS. The DHCS is acting on behalf of CDSS for purposes of receiving reports of privacy and information security incidents and breaches. The County Department/Agency agrees to perform the following incident reporting to DHCS:

1. If a suspected security incident involves PII provided or verified by SSA, the County Department/Agency shall immediately notify DHCS upon discovery. For more information on SSA data, please see the Definition section of this Agreement.

2. If a suspected security incident does not involve PII provided or verified by SSA, the County Department/Agency shall notify DHCS within one (1) working day of discovery.

If it is unclear if the security incident involves SSA data, the County Department/Agency shall immediately report the incident upon discovery.

A County Department/Agency shall notify DHCS of all personal information, as defined by California Civil Code Section 1798.3(a), that may have been accessed, used, or disclosed in any suspected security incident or breach, including but not limited to case numbers.

Notice shall be made using the DHCS Privacy Incident Report (PIR) form, including all information known at the time. The County Department/Agency shall use the most current version of this form, which is available on the DHCS Privacy Office website at: http://www.dhcs.ca.gov/formsandpubs/laws/priv/Pages/CountiesOnly.aspx. All PIRs and supporting documentation are to be submitted to DHCS via email using the "DHCS Breach and Security Incidents Reporting" contact information found below in Subsection F.

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

Upon discovery of a breach, security incident, intrusion, or unauthorized access, use, or disclosure of PII, the County Department/Agency shall take:

1. Prompt action to mitigate any risks or damages involved with the occurrence and to protect the operating environment; and
2. Any action pertaining to such occurrence required by applicable Federal and State laws and regulations.

B. Investigation and Investigative Report. The County Department/Agency shall immediately investigate breaches and security incidents involving PII. If the initial PIR was submitted incomplete and if new or updated information is available, submit an updated PIR to DHCS within seventy-two (72) hours of the discovery. The updated PIR shall include any other applicable information related to the breach or security incident known at that time.

C. ***Complete*** Report. If all of the required information was not included in either the initial report or the investigation PIR submission, then a separate complete report shall be submitted within ten working days of the discovery. The Complete Report of the investigation shall include an assessment of all known factors relevant to the determination of whether a breach occurred under applicable provisions of the Health Insurance Portability and Accountability Act (HIPAA), the Health Information Technology for Economic and Clinical Health (HITECH) Act, the Information Protection Act, or other applicable law. The report shall also include a Corrective Action Plan (CAP) that shall include, at minimum, detailed information regarding the mitigation measures taken to halt and/or contain the improper use or disclosure.

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

D. ***Notification of Individuals***. When applicable state or federal law requires notification to individuals of a breach or unauthorized disclosure of their PII, the County Department/Agency shall give the notice, subject to the following provisions:

   1. If the cause of the breach is attributable to the County Department/Agency or its subcontractors, agents or vendors, the County Department/Agency shall pay any costs of such notifications, as well as any and all costs associated with the breach. If the cause of the breach is attributable to CDSS, CDSS shall pay any costs associated with such notifications, as well as any costs associated with the breach. If there is any question as to whether CDSS or the County Department/Agency is responsible for the breach, CDSS and the County Department/Agency shall jointly determine responsibility for purposes of allocating the costs;

2. All notifications (regardless of breach status) regarding beneficiaries' PII shall comply with the requirements set forth in Section 1798.29 of the California Civil Code and Section 17932 of Title 42 of United States Code, inclusive of its implementing regulations, including but not limited to the requirement that the notifications be made without unreasonable delay and in no event, later than sixty (60) calendar days from discovery;
3. The CDSS Information Security and Privacy Bureau shall approve the time, manner and content of any such notifications and their review and approval shall be obtained before notifications are made. If notifications are distributed without CDSS review and approval, secondary follow-up notifications may be required; and
4. CDSS may elect to assume responsibility for such notification from the County Department/Agency.

E. ***Responsibility for Reporting of Breaches when Required by State or Federal Law***. If the cause of a breach is attributable to the County Department/Agency or its agents, subcontractors or vendors, the County Department/Agency is responsible for all required reporting of the breach. If the cause of the breach is attributable to CDSS, CDSS is responsible for all required reporting of the breach. When applicable law requires the breach be reported to a federal or state agency or that notice be given to media outlets, DHCS (if the breach involves MEDS or SSA data), CDSS, and the County Department/Agency shall coordinate to ensure such reporting is in compliance with applicable law and to prevent duplicate reporting, and to jointly determine responsibility for purposes of allocating the costs of such reports, if any.

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

CDSS Information Security and Privacy Bureau	DHCS Breach and Security Incident Reporting
California Department of Social Services Information Security and Privacy Bureau 744 P Street, MS 9-9-70 Sacramento, CA 95814-6413 Email: iso@dss.ca.gov Telephone: (916) 651-5558 *The preferred method of communication is email, when available. Do not include any PII unless requested by CDSS.*	Department of Health Care Services Office of HIPAA Compliance 1501 Capitol Avenue, MS 4721 P.O. Box 997413 Sacramento, CA 95899-7413 Email: incidents@dhcs.ca.gov Telephone: (866) 866-0602 *The preferred method of communication is email, when available. Do not include any Medi-Cal PII unless requested by DHCS.*

XI. COMPLIANCE WITH SSA AGREEMENT

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

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

If SSA changes the terms of its agreement(s) with CDSS, CDSS will, as soon as reasonably possible after receipt, supply copies to the County Welfare Directors Association (CWDA) as well as the proposed target date for compliance. For a period of thirty (30) days, CDSS will accept input from CWDA on the proposed target date and make adjustments, if appropriate. After the thirty (30) day period, CDSS will submit the proposed target date to SSA, which will be subject to adjustment by SSA. Once a target date for compliance is determined by SSA, CDSS will supply copies of the changed agreement to the CWDA and the County Department/Agency, along with the compliance date expected by SSA. If the County Department/Agency is not able to meet the SSA compliance date, it shall submit a CAP to CDSS for review and approval at least thirty (30) days prior to the SSA compliance date. Any potential County Department/Agency resource issues may be discussed with CDSS through a collaborative process in developing their CAP.

A copy of Exhibit A can be requested by authorized County Department/Agency individuals by emailing CDSS at cdsspsa@dss.ca.gov.

XII. COMPLIANCE WITH DEPARTMENT OF HOMELAND SECURITY AGREEMENT

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

If DHS-USCIS changes the terms of its agreement(s) with CDSS, CDSS will, as soon as reasonably possible after receipt, supply copies to CWDA as well as the CDSS proposed target date for compliance. For a period of thirty (30) days, CDSS will accept input from CWDA on the proposed target date and make adjustments, if appropriate. After the thirty (30) day period, CDSS will submit the proposed target date to DHS-USCIS, which will be subject to adjustment by DHS-USCIS. Once a target date for compliance is determined by DHS-USCIS, CDSS will supply copies of the changed agreement to the CWDA and the County Department/Agency, along with the compliance date expected by DHS-USCIS. If a County Department/Agency is not able to meet the DHS-USCIS compliance date, it shall submit a CAP to CDSS for review and approval at least thirty (30) days prior to the DHS-USCIS compliance date. Any potential County Department/Agency resource issues may be discussed with CDSS through a collaborative process in developing their CAP.

A copy of Exhibit B can be requested by authorized County Department/Agency individuals by emailing CDSS at cdsspsa@dss.ca.gov.

XIII. COUNTY DEPARTMENT/AGENCY AGENTS, SUBCONTRACTORS, AND VENDORS

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

County Department/Agency(s) who would like assistance or guidance with this requirement are encouraged to contact CDSS via email at cdsspsa@dss.ca.gov.

XIV. ASSESSMENTS AND REVIEWS

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

XV. ASSISTANCE IN LITIGATION OR ADMINISTRATIVE PROCEEDINGS

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

XVI. AMENDMENT OF AGREEMENT

The CDSS and the County Department/Agency acknowledge that federal and state laws relating to data security and privacy are rapidly evolving and that an amendment to this Agreement may be required to ensure compliance with all data security and privacy procedures. Upon request by CDSS, the County Department/Agency agrees to promptly enter into negotiations with CDSS concerning an amendment to this Agreement as may be needed by developments in federal and state laws and regulations. In addition to any other lawful remedy, CDSS may terminate this Agreement upon thirty (30) days written notice if the County Department/Agency does not promptly agree to enter into negotiations to amend this Agreement when requested to do so, or does not enter into an amendment that CDSS deems necessary.

Each amendment shall be properly identified as Agreement No., Amendment No. (A-1, A-2, A-3, etc.) to identify the applicable changes to this Agreement, and be effective upon execution by the parties.

XVII. TERM OF AGREEMENT

The term of this agreement shall begin upon signature and approval of CDSS.

XVIII. TERMINATION

A. This Agreement shall terminate on **September 1, 2022**, regardless of the date the Agreement is executed by the parties. The parties can agree in writing to extend the term of the Agreement; through an executed written amendment. County Department/Agency requests for an extension shall be justified and approved by CDSS and limited to no more than a six (6) month extension.

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

XIX. TERMINATION FOR CAUSE

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

XX. SIGNATORIES

The signatories below warrant and represent that they have the competent authority on behalf of their respective agencies to enter into the obligations set forth in this Agreement.

The authorized officials whose signatures appear below have committed their respective agencies to the terms of this Agreement. The contract is effective on **September 1, 2019**.

For the County of_____

Department/Agency of _____,

_____	_____
(Signature)	(Date)
_____	_____
(Name – Print or Type)	(Title – Print or Type)

For the California Department of Social Services,

_____	_____
(Signature)	(Date)
_____	Chief, Contracts & Purchasing Bureau
(Name – Print or Type)	(Title – Print or Type)

EXHIBIT A

Exhibit A consists of the current versions of the following documents, copies of which can be requested by the County Department/Agency information security and privacy staff from CDSS by emailing CDSS at cdsspsa@dss.ca.gov.

- Computer Matching and Privacy Protection Act Agreement between the SSA and California Health and Human Services Agency
- Information Exchange Agreement between SSA and CDSS (IEA-F and IEA-S)
- Electronic Information Exchange Security Requirements and Procedures for State and Local Agencies Exchanging Electronic Information with the SSA (TSSR)

EXHIBIT B

Exhibit B consists of the current version of the following document, a copy of which can be requested by the County Department/Agency information security and privacy staff by emailing CDSS at cdsspsa@dss.ca.gov.

- Computer Matching Agreement between the Department of Homeland Security, United States Citizenship and Immigration Services (DHS-USCIS) and California Department of Social Services (CA-DSS)

MEDI-CAL PRIVACY & SECURITY AGREEMENT NO.: 24 - 19

MEDI-CAL PRIVACY AND SECURITY AGREEMENT

BETWEEN

the California Department of Health Care Services and the

County of Los Angeles,

Department/Agency of

Public Social Services.

PREAMBLE

The Department of Health Care Services (DHCS) and the

County of Los Angeles,

Department/Agency of Public Social Services

(County Department) enter into this Medi-Cal Privacy and Security Agreement (Agreement) in order to ensure the privacy and security of Medi-Cal Personally Identifiable Information (Medi-Cal PII).

DHCS receives federal funding to administer California's Medicaid Program (Medi-Cal). The County Department/Agency assists in the administration of Medi-Cal, in that DHCS and the County Department/Agency access DHCS eligibility information for the purpose of determining Medi-Cal eligibility.

This Agreement covers the

County of Los Angeles,

Department/Agency of Public Social Services

workers, who assist in the administration of Medi-Cal; and access, use, or disclose Medi-Cal PII.

DEFINITIONS

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

1. **"Assist in the administration of the Medi-Cal program"** means performing administrative functions on behalf of Medi-Cal, such as establishing eligibility, determining the amount of medical assistance, and collecting Medi-Cal PII for such purposes, to the extent such activities are authorized by law.

2. **"Breach"** refers to actual loss, loss of control, compromise, unauthorized disclosure,

unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for other than authorized purposes have access or potential access to Medi-Cal PII, whether electronic, paper, verbal, or recorded.

3. **"County Worker"** means those county employees, contractors, subcontractors, vendors and agents performing any functions for the County that require access to and/or use of Medi-Cal PII and that are authorized by the County to access and use Medi-Cal PII. An agent is a person or organization authorized to act on behalf of the County Department/Agency.

4. **"Medi-Cal PII"** is information directly obtained in the course of performing an administrative function on behalf of Medi-Cal that can be used alone, or in conjunction with any other information, to identify a specific individual. Medi-Cal PII includes any information that can be used to search for or identify individuals, or can be used to access their files, including but not limited to name, social security number (SSN), date and place of birth (DOB), mother's maiden name, driver's license number, or identification number. Medi-Cal PII may also include any information that is linkable to an individual, such as medical, educational, financial, and employment information. Medi-Cal PII may be electronic, paper, verbal, or recorded and includes statements made by, or attributed to, the individual.

5. **"Security Incident"** means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of Medi-Cal PII, or interference with system operations in an information system which processes Medi-Cal PII that is under the control of the County or California Statewide Automated Welfare System (CalSAWS) Consortium, or a contractor, subcontractor or vendor of the County.

6. **"Secure Areas"** means any area where:
   A. County Workers assist in the administration of Medi-Cal;
   B. County Workers use or disclose Medi-Cal PII; or
   C. Medi-Cal PII is stored in paper or electronic format.

7. **"SSA-provided or verified data (SSA data)"** means:
   A. Any information under the control of the Social Security Administration (SSA) provided to DHCS under the terms of an information exchange agreement with SSA (e.g., SSA provided date of death, SSA Title II or Title XVI benefit and eligibility data, or SSA citizenship verification); or

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

MEDI-CAL PRIVACY & SECURITY AGREEMENT NO.: 24 - 19

AGREEMENTS

DHCS and County Department/Agency mutually agree as follows:

I. PRIVACY AND CONFIDENTIALITY

A. County Department/Agency County Workers may use or disclose Medi-Cal PII only as permitted in this Agreement and only to assist in the administration of Medi-Cal in accordance with Section 14100.2 of the Welfare and Institutions Code, Section 431.302 of Title 42 Code of Federal Regulations, as limited by this Agreement, and as otherwise required by law. Disclosures required by law or that are made with the explicit written authorization of a Medi-Cal client, such as through an authorized release of information form, are allowable. Any other use or disclosure of Medi-Cal PII requires the express approval in writing of DHCS. No County Worker shall duplicate, disseminate or disclose Medi-Cal PII except as allowed in this Agreement.

B. While DHCS is a covered entity under the federal Health Insurance Portability and Accountability Act, as amended from time to time (HIPAA), the County Department/Agency is not required to be the business associate of DHCS, if the activities of the County Department/Agency are limited to determining eligibility for, or enrollment in, Medi-Cal (45 CFR 160.103). Nevertheless, it is the intention of the parties to protect the privacy and security of Medi-Cal PII and the rights of Medi-Cal applicants and beneficiaries in a manner that is consistent with HIPAA and other laws that are applicable. It is not the intention of the parties to voluntarily subject the County Department/Agency to federal HIPAA jurisdiction where it would not otherwise apply, and DHCS does not assert any authority to do so.

1. To the extent that other state and/or federal laws provide additional, stricter, and/or more protective (collectively, more protective) privacy and/or security protections to Medi-Cal PII covered under this Agreement beyond those provided through HIPAA, as applicable, County Department/Agency shall:

   a. Comply with the more protective of the privacy and security standards set forth in applicable state or federal laws to the extent such standards provide a greater degree of protection and security than HIPAA or are otherwise more favorable to the individuals whose information is concerned; and

   b. Treat any violation of such additional and/or more protective standards as a breach or security incident, as appropriate, pursuant to Section VIII. of this Agreement. It is not the intention of the parties that this subsection I.B.(1)(b) expands the definitions of breach nor security incident set forth this Agreement unless the additional and/or more protective standard has a different definition

for these terms, as applicable.

Examples of laws that provide additional and/or stricter privacy protections to certain types of Medi-Cal PII include, but are not limited to the Confidentiality of Alcohol and Drug Abuse Patient Records, 42 CFR Part 2, Welfare and Institutions Code section 5328, and California Health and Safety Code section 11845.5.

C. Access to Medi-Cal PII shall be restricted to County Workers who need to perform their official duties to assist in the administration of Medi-Cal.

D. County Workers who access, disclose or use Medi-Cal PII in a manner or for a purpose not authorized by this Agreement may be subject to civil and criminal sanctions contained in applicable federal and state statutes.

II. PERSONNEL CONTROLS

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

A. ***Employee Training.*** Train and use reasonable measures to ensure compliance with the requirements of this Agreement by County Workers, including, but not limited to:

1. Provide initial privacy and security awareness training to each new County Worker within 30 days of employment;

2. Thereafter, provide annual refresher training or reminders of the privacy and security safeguards in this Agreement to all County Workers. Three or more security reminders per year are recommended;

3. Maintain records indicating each County Worker's name and the date on which the privacy and security awareness training was completed and;

4. Retain training records for a period of five years after completion of the training.

B. ***Employee Discipline***.

1. Provide documented sanction policies and procedures for County Workers who fail to comply with privacy policies and procedures or any provisions of these requirements.

2. Sanction policies and procedures shall include termination of employment

when appropriate.

C. ***Confidentiality Statement***. Ensure that all County Workers sign a confidentiality statement. The statement shall be signed by County Workers prior to accessing Medi-Cal PII and annually thereafter. Signatures may be physical or electronic. The signed statement shall be retained for a period of five years.

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

1. General Use of Medi-Cal PII;
2. Security and Privacy Safeguards for Medi-Cal PII;
3. Unacceptable Use of Medi-Cal PII; and
4. Enforcement Policies.

D. ***Background Screening.***

1. Conduct a background screening of a County Worker before they may access Medi-Cal PII.

2. The background screening should be commensurate with the risk and magnitude of harm the employee could cause. More thorough screening shall be done for those employees who are authorized to bypass significant technical and operational security controls.

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

III. MANAGEMENT OVERSIGHT AND MONITORING

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

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

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

B. Utilize Medi-Cal Eligibility Data System (MEDS) audit reports provided by DHCS and other system auditing tools available to County Department/Agency to perform quality assurance and management oversight

reviews of their County Workers' access to Medi-Cal and SSA PII within data systems utilized, including MEDS. For additional information see Medi-Cal Eligibility Division Information Letter | 21-34. Any instances of suspected security incidents or breaches are to be reported to DHCS immediately following the instructions within Section X of this Agreement.

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

IV. INFORMATION SECURITY AND PRIVACY STAFFING

The County Department/Agency agrees to:

A. Designate information security and privacy officials who are accountable for compliance with these and all other applicable requirements stated in this Agreement.

B. Provide the DHCS with applicable contact information for these designated individuals using the County PSA inbox listed in Section IX of this Agreement. Any changes to this information should be reported to DHCS within ten days.

C. Assign County Workers to be responsible for administration and monitoring of all security-related controls stated in this Agreement.

V. TECHNICAL SECURITY CONTROLS

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

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

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

DHCS and CDSS will enter into a separate PSA with California Statewide Automated Welfare System (CalSAWS) Joint Powers Authority specific to the CalSAWS. Any requirements for data systems in this PSA would only apply to County Department/Agency's locally operated/administered systems that access, store, or process Medi-Cal PII.

A. Systems Security Standards and Requirements

1. **Access Control (AC)**

Control Number	AC-1
Title	Access Control Policy and Procedures
DHCS Requirement	The organization must: a. Develop, document, and disseminate to designated organization officials: 1. An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; 2. Procedures to facilitate the implementation of the access control policy and associated access control controls; b. Review and update the current access control procedures with the organization-defined frequency.
Supplemental Guidance (from NIST 800-53)	This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the AC family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.
Control Number	AC-2
Title	Account Management
DHCS Requirement	The organization must: a. Identify and select the accounts with access to Medi-Cal PII to support organizational missions/business functions. b. Assign account managers for information system accounts; c. Establish conditions for group and role membership; d. Specify authorized users of the information system, group and role membership, and access
	authorizations (i.e., privileges) and other attributes (as required) for each account; e. Require approvals by designated access authority for requests to create information system accounts; f. Create, enable, modify, disable, and remove information system accounts in accordance with organization account management procedures; g. Monitors the use of information system accounts; h. Notifies account managers when accounts are no longer required, when users are terminated or transferred; and when individual information system usage or need-to-know changes. i. Authorizes access to the information systems that receive, process, store or transmit Medi-Cal PII based on valid access authorization, need-to-know permission or under the authority to re-disclose Medi-Cal PII. j. Review accounts for compliance with account management requirements according to organization-based frequency; and k. Establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.
Supplemental Guidance (from NIST 800-53)	Information system account types include, for example, individual, shared, group, system, guest/anonymous, emergency, developer/manufacturer/vendor, temporary, and service. Some of the account management requirements listed above can be implemented by organizational information systems. The identification of authorized users of the information system and the specification of access privileges reflects the requirements in other security controls in the security plan. Users requiring administrative privileges on information system accounts receive additional scrutiny by appropriate organizational personnel (e.g., system owner, mission/business owner, or chief information security officer) responsible for approving such accounts and privileged access. Organizations may choose to define access privileges or other attributes by account, by type of account, or a combination of both. Other attributes required for authorizing access include, for example, restrictions on time-of-day, day-of-week, and point-of-origin. In defining other account attributes, organizations consider system-related requirements (e.g., scheduled maintenance, system upgrades) and mission/business requirements, (e.g., time zone differences, customer requirements, remote access to support travel requirements). Failure to consider these factors could affect information system availability. Temporary and emergency accounts are accounts intended for short-term use. Organizations establish temporary accounts as a part of normal account activation procedures when there is a need for short-term accounts without the demand for immediacy in account activation. Organizations establish emergency accounts in response to crisis situations and with the need for rapid account activation. Therefore, emergency account activation may bypass normal account authorization processes. Emergency and temporary accounts are not to be confused with infrequently used accounts (e.g., local logon accounts used for special tasks defined by organizations or when network resources are unavailable). Such accounts remain available and are not subject to automatic disabling or removal dates. Conditions for disabling or deactivating accounts include, for example: (i) when shared/group, emergency, or temporary accounts are no longer required; or (ii) when individuals are transferred or terminated. Some types of information system accounts may require specialized training. Related controls: AC-3, AC-4, AC-5, AC-6, AC-10, AC-17, AC-19, AC-20, AU-9, IA-2, IA-4, IA-5, IA-8, CM-5, CM-6, CM-11, MA-3, MA-4, MA-5, PL-4, SC-13.

Control Number	AC-3
Title	Access Enforcement
DHCS Requirement	The organization must: Enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.
Supplemental Guidance	Access control policies (e.g., identity-based policies, role-based policies, control matrices, cryptography) control access between active entities or subjects (i.e., users or processes acting on behalf of users) and passive entities or objects (e.g., devices, files, records, domains) in information systems. In addition to enforcing authorized access at the information system level and recognizing that information systems can host many applications and services in support of organizational missions and business operations, access enforcement mechanisms can also be employed at the application and service level to provide increased information security. Related controls: AC-2, AC-4, AC-5, AC-6, AC-16, AC-17, AC-
Control Number	AC-3(7)
Title	Access Enforcement | Role-Based Access Control
DHCS Requirement	The organization information system must: enforce a role-based access control policy over defined subjects and objects and controls access based upon the need to utilize Medi-Cal PII.
Supplemental Guidance (from NIST 800-53)	Role-based access control (RBAC) is an access control policy that restricts information system access to authorized users. Organizations can create specific roles based on job functions and the authorizations (i.e., privileges) to perform needed operations on organizational information systems associated with the organization-defined roles. When users are assigned to the organizational roles, they inherit the authorizations or privileges defined for those roles. RBAC
	simplifies privilege administration for organizations because privileges are not assigned directly to every user (which can be a significant number of individuals for mid- to large-size organizations) but are instead acquired through role assignments. RBAC can be implemented either as a mandatory or discretionary form of access control. For organizations implementing RBAC with mandatory access controls, the requirements in AC-3 (3) define the scope of the subjects and objects covered by the policy.
Control Number	AC-3(8)
Title	Access Enforcement | Revocation of Access Authorization
DHCS Requirement	The organization must: Enforce a role-based access control over users and information resources that have access to Medi-Cal PII, and control access based upon organization defined roles and users authorized to assume such roles.
Supplemental Guidance (from NIST 800-53)	Revocation of access rules may differ based on the types of access revoked. For example, if a subject (i.e., user or process) is removed from a group, access may not be revoked until the next time the object (e.g., file) is opened or until the next time the subject attempts a new access to the object. Revocation based on changes to security labels may take effect immediately. Organizations can provide alternative approaches on how to make revocations immediate if information systems cannot provide such capability and immediate revocation is necessary.
Control Number	AC-4
Title	Information Flow Enforcement
DHCS Requirement	The organization information system must: enforce approved authorizations for controlling the flow of information within the system and between interconnected systems based on the need for interconnected systems to share Medi-Cal PII to conduct business.
Supplemental Guidance (from NIST 800-53)	Information flow control regulates where information is allowed to travel within an information system and between information systems (as opposed to who is allowed to access the information) and without explicit regard to subsequent accesses to that information. Flow control restrictions include, for example, keeping export-controlled information from being transmitted in the clear to the Internet, blocking outside traffic that claims to be from within the organization, restricting web requests to the Internet that are not from the internal web proxy server, and limiting information transfers between organizations based on data structures and content. Transferring information between information systems representing different security domains with different security policies introduces risk that such transfers violate one or more domain security policies. In such situations, information owners/stewards provide guidance at designated policy enforcement points between interconnected systems. Organizations consider mandating specific architectural solutions when required to enforce specific security policies. Enforcement includes, for example: (i) prohibiting information transfers between interconnected systems (i.e., allowing access only); (ii) employing hardware mechanisms to enforce one-way information flows; and (iii) implementing trustworthy regrading mechanisms to reassign security attributes and security labels. Organizations commonly employ information flow control policies and enforcement mechanisms to control the flow of information between designated sources and destinations (e.g., networks, individuals, and devices) within information systems and between interconnected systems. Flow control is based on the characteristics of the information and/or the information path. Enforcement occurs, for example, in boundary protection devices (e.g., gateways, routers, guards, encrypted tunnels, firewalls) that employ rule sets or establish configuration settings that restrict information system services, provide a packet-filtering capability based on header information, or message- filtering capability based on message content (e.g., implementing key word searches or using document characteristics). Organizations also consider the trustworthiness of filtering/inspection mechanisms (i.e., hardware, firmware, and software components) that are critical to information flow enforcement. Control enhancements 3 through 22 primarily address cross-domain solution needs which focus on more advanced filtering techniques, in-depth analysis, and stronger flow enforcement mechanisms implemented in cross-domain products, for example, high-assurance guards. Such capabilities are generally not available in commercial off-the-shelf information technology products. Related controls: AC-3, AC-17, AC-19, AC-21, CM-6, CM-7, SA-8, SC-2, SC-5, SC-7, SC-18

Control Number	AC-5
Title	Separation of Duties
DHCS Requirement	The organization must: a. Separate organization-defined duties of individuals; b. Document separation of duties of individuals; and c. Defines information system access authorizations to support separation of duties. *DHCS also requires that the state organization prohibit any functional component(s) or official(s) from issuing credentials or access authority to themselves or other individuals within their job-function or category of access.* *Federal requirements and DHCS policy exclude any employee who uses Medi-Cal PII to process programmatic workloads to make benefit or entitlement determinations from participation in management or quality assurance functions.*
Supplemental Guidance (from NIST 800-53)	Separation of duties addresses the potential for abuse of authorized privileges and helps to reduce the risk of malevolent activity without collusion. Separation of duties includes, for example: (i) dividing mission functions and information system support functions among different individuals and/or roles; (ii) conducting information system support functions with different individuals (e.g., system management, programming, configuration management, quality assurance and testing, and network security); and (iii) ensuring security personnel administering access control functions do not also administer audit functions. Related controls: AC-3, AC-6, PE-3, PE-4, PS-2.
Control Number	AC-6
Title	Least Privilege
DHCS Requirement	The organization must: Employ the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.
Supplemental Guidance (from NIST 800-53)	Organizations employ least privilege for specific duties and information systems. The principle of least privilege is also applied to information system processes, ensuring that the processes operate at privilege levels no higher than necessary to accomplish required organizational missions/business functions. Organizations consider the creation of additional processes, roles, and information system accounts as necessary, to achieve least privilege. Organizations also apply least privilege to the development, implementation, and operation of organizational information systems. Related controls: AC-2, AC-3, AC-5, CM-6, CM-7, PL-2.
Control Number	AC-6(1)
Title	Least Privilege | Authorize Access to Security Functions
DHCS Requirement	The organization must explicitly authorize access to organization-defined security functions (deployed in hardware, software, and firmware) and security-relevant information.
Supplemental Guidance (from NIST 800-53)	Security functions include, for example, establishing system accounts, configuring access authorizations (i.e., permissions, privileges), setting events to be audited, and setting intrusion detection parameters. Security-relevant information includes, for example, filtering rules for routers/firewalls, cryptographic key management information, configuration parameters for security services, and access control lists. Explicitly authorized personnel include, for example, security administrators, system and network administrators, system security officers, system maintenance personnel, system programmers, and other privileged users.
Control Number	AC-6(7)
Title	Least Privilege | Review Of User Privileges
DHCS Requirement	The organization must: a. Review the privileges assigned to organization-defined roles or classes of users to validate the need for such privileges; and b. Reassign or removes privileges, if necessary, to correctly reflect organizational mission/business needs.
Supplemental Guidance (from NIST 800-53)	The need for certain assigned user privileges may change over time reflecting changes in organizational missions/business function, environments of operation, technologies, or threat. Periodic review of assigned user privileges is necessary to determine if the rationale for assigning such privileges remains valid. If the need cannot be revalidated, organizations take appropriate corrective actions. Related control: CA-7.
Control Number	AC-7
Title	Unsuccessful Logon Attempts
DHCS Requirement	The organization must: a. Enforce a limit of no fewer than three (3) and no greater than five (5) consecutive invalid logon attempts by a user during an organization-defined time period; and b. Automatically lock the account/node for: an organization-defined time period; or locks the account/node until released by an administrator; or delays next logon prompt according to organization-defined delay algorithm when the maximum number of unsuccessful attempts is exceeded.
Supplemental Guidance (from NIST 800-53)	This control applies regardless of whether the logon occurs via a local or network connection. Due to the potential for denial of service, automatic lockouts initiated by information systems are usually temporary and automatically release after a predetermined time period established by organizations. If a delay algorithm is selected, organizations may choose to employ different algorithms for different information system components based on the capabilities of those components. Responses to unsuccessful logon attempts may be implemented at both the operating system and the application levels. Related controls: AC-2, AC-9, AC-14, IA-5.

Control Number	AC-8
Title	System Use Notification
DHCS Requirement	The organization must: a. Displays to users system use notification message or banner before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance and states that: 1. Users are accessing a U.S. Government information system; 2. Information system usage may be monitored, recorded, and subject to audit; 3. Unauthorized use of the information system is prohibited and subject to criminal and civil penalties; and 4. Use of the information system indicates consent to monitoring and recording; b. Retains the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the information system; and c. For publicly accessible systems: 1. Displays system use information organization-defined conditions, before granting further access; 2. Displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and 3. Includes a description of the authorized uses of the system. At a minimum, this can be done at initial logon and is not required for every logon.
Supplemental Guidance (from NIST 800-53)	System use notifications can be implemented using messages or warning banners displayed before individuals log in to information systems. System use notifications are used only for access via logon interfaces with human users and are not required when such human interfaces do not exist. Organizations consider system use notification messages/banners displayed in multiple languages based on specific organizational needs and the demographics of information system users. Organizations also consult with the Office of the General Counsel for legal review and approval of warning banner content.
Control Number	AC-11
Title	Session Lock
DHCS Requirement	The organization's information system: a. Prevents further access to the system by initiating a session lock after 15 minutes or upon receiving a request from a user; and b. Retains the session lock until the user reestablishes access using established identification and authentication procedures.
Supplemental Guidance (from NIST 800-53)	Session locks are temporary actions taken when users stop work and move away from the immediate vicinity of information systems but do not want to log out because of the temporary nature of their absences. Session locks are implemented where session activities can be determined. This is typically at the operating system level, but can also be at the application level. Session locks are not an acceptable substitute for logging out of information systems, for example, if organizations require users to log out at the end of workdays. Related control: AC-7.
Control Number	AC-17
Title	Remote Access
DHCS Requirement	The organization must: a. Establish and document usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; and b. Authorize remote access to the information system prior to allowing such connections.
Supplemental Guidance (from NIST 800-53)	Remote access is access to organizational information systems by users (or processes acting on behalf of users) communicating through external networks (e.g., the Internet). Remote access methods include, for example, dial-up, broadband, and wireless. Organizations often employ encrypted virtual private networks (VPNs) to enhance confidentiality and integrity over remote connections. The use of encrypted VPNs does not make the access non-remote; however, the use of VPNs, when adequately provisioned with appropriate security controls (e.g., employing appropriate encryption techniques for confidentiality and integrity protection) may provide sufficient assurance to the organization that it can effectively treat such connections as internal networks. Still, VPN connections traverse external networks, and the encrypted VPN does not enhance the availability of remote connections. Also, VPNs with encrypted tunnels can affect the organizational capability to adequately monitor network communications traffic for malicious code. Remote access controls apply to information systems other than public web servers or systems designed for public access. This control addresses authorization prior to allowing remote access without specifying the formats for such authorization. While organizations may use interconnection security agreements to authorize remote access connections, such agreements are not required by this control. Enforcing access restrictions for remote connections is addressed in AC-3. Related controls: AC-2, AC-3, AC-18, AC-19, AC-20, CA-3, CA-7, CM-8, IA-2, IA-3, IA-8, MA-4, PE-17, PL-4, SC-10, SI-4.

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

Control Number	AR-3
Title	Privacy Requirements for Contractors and Service Providers
DHCS Requirement	The organization must: a. Establish privacy roles, responsibilities, and access requirements for contractors and service providers; and b. Includes privacy requirements in contracts and other acquisition-related documents.
Supplemental Guidance (from NIST 800-53)	Contractors and service providers include, but are not limited to, information providers, information processors, and other organizations providing information system development, information technology services, and other outsourced applications. Organizations consult with legal counsel, the Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO), and contracting officers about applicable laws, directives, policies, or regulations that may impact implementation of this control. Related control: AR-1, AR-5, SA-4.

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

Control Number	AU-1
Title	Audit and Accountability Policy and Procedures
DHCS Requirement	The organization must: a. Develop, document, and disseminate to individuals and organizations that store, process, or transmit Medi-Cal PII: 1. An audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls; and b. Review and update the current: 1. Audit and accountability policy at least triennially; and 2. Audit and accountability procedures at least triennially.
Supplemental Guidance (from NIST 800-53)	This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the AU family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.
Control Number	AU-2
Title	Audit Events
DHCS Requirement	The organization must: a. Audit the following events: 1) Viewing Medi-Cal PII stored within the organization's system; 2) Viewing of screens that contain Medi-Cal PII; 3) All system and data interactions concerning Medi-Cal PII. b. Coordinate the security audit function with other organizational entities requiring audit-related information to enhance mutual support and to help guide the selection of auditable events; c. Determines that the following events are to be audited within the information system: 1) Viewing Medi-Cal PII stored within the organization's system; 2) Viewing of screens that contain Medi-Cal PII; 3) All system and data interactions concerning Medi-Cal PII.
Supplemental Guidance (from NIST 800-53)	An event is any observable occurrence in an organizational information system. Organizations identify audit events as those events which are significant and relevant to the security of information systems and the environments in which those systems operate in order to meet specific and ongoing audit needs. Audit events can include, for example, password changes, failed logons, or failed accesses related to information systems, administrative privilege usage, PIV credential usage, or third-party credential usage. In determining the set of auditable events, organizations consider the auditing appropriate for each of the security controls to be implemented. To balance auditing requirements with other information system needs, this control also requires identifying that subset of auditable events that are audited at a given point in time. For example, organizations may determine that information systems must have the capability to log every file access both successful and unsuccessful, but not activate that capability except for specific circumstances due to the potential burden on system performance. Auditing requirements, including the need for auditable events, may be referenced in other security controls and control enhancements. Organizations also include auditable events that are required by applicable federal laws, Executive Orders, directives, policies, regulations, and standards. Audit records can be generated at various levels of abstraction, including at the packet level as information traverses the network. Selecting the appropriate level of abstraction is a critical aspect of an audit capability and can facilitate the identification of root causes to problems. Organizations consider in the definition of auditable events, the auditing necessary to cover related events such as the steps in distributed, transaction-based processes (e.g., processes that are distributed across multiple organizations) and actions that occur in service-oriented architectures. Related controls: AC-6, AC-17, AU-3, AU-12, MA-4, MP-2, MP-4, SI-4

Control Number	AU-11
Title	Audit Record Retention
DHCS Requirement	The organization must retain audit records for six (6) years to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.
Supplemental Guidance (from NIST 800-53)	Organizations retain audit records until it is determined that they are no longer needed for administrative, legal, audit, or other operational purposes. This includes, for example, retention and availability of audit records relative to Freedom of Information Act (FOIA) requests, subpoenas, and law enforcement actions. Organizations develop standard categories of audit records relative to such types of actions and standard response processes for each type of action. The National Archives and Records Administration (NARA) General Records Schedules provide federal policy on record retention. Related controls: AU-4, AU-5, AU-9, MP-6.
Control Number	AU-12
Title	Audit Generation
DHCS Requirement	The organization information system must: a. Provide audit record generation capability for the auditable events defined in AU-2 a. at the audit reporting mechanism; b. Allow security personnel to select which auditable events are to be audited by specific components of the information system; and c. Generates audit records for the events defined in AU-2 d. with the content defined in AU-3
Supplemental Guidance (from NIST 800-53)	Audit records can be generated from many different information system components. The list of audited events is the set of events for which audits are to be generated. These events are typically a subset of all events for which the information system is capable of generating audit records. Related controls: AC-3, AU-2, AU-3, AU-6, AU-7.

4. Awareness and Training (AT)

Control Number	AT-1
Title	Security Awareness and Training Policy and Procedures
DHCS Requirement	The organization must: a. Develop, document, and disseminate to personnel and organizations with access to Medi-Cal PII: 1. A security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls; and b. Reviews and updates the current: 1. Security awareness and training policy and; 2. Security awareness and training procedures. The training and awareness programs must include: The sensitivity of Medi-Cal PII, The rules of behavior concerning use and security in systems and/or applications processing Medi-Cal PII, The Privacy Act and other Federal and state laws, including but not limited to Section 14100.2 of the Welfare and Institutions Code and Section 431.302 et. Seq. of Title 42 Code of Federal Regulations, governing collection, maintenance, use, and dissemination of information about individuals, The possible criminal and civil sanctions and penalties for misuse of Medi-Cal PII, The responsibilities of employees, contractors, and agent's pertaining to the proper use and protection of Medi-Cal PII, The restrictions on viewing and/or copying Medi-Cal PII, The proper disposal of Medi-Cal PII, The security breach and data loss incident reporting procedures, The basic understanding of procedures to protect the network from viruses, worms, Trojan horses, and other malicious code, Social engineering (phishing, vishing and pharming) and network fraud prevention.
Supplemental Guidance (from NIST 800-53)	This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the AT family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, tandards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.

Control Number	AT-2
Title	Security Awareness Training
DHCS Requirement	The organization must provide basic security awareness training to information system users (including managers, senior executives, and contractors): a. As part of initial training for new users; b. When required by information system changes; and c. Annually thereafter.
Supplemental Guidance (from NIST 800-53)	Organizations determine the appropriate content of security awareness training and security awareness techniques based on the specific organizational requirements and the information systems to which personnel have authorized access. The content includes a basic understanding of the need for information security and user actions to maintain security and to respond to suspected security incidents. The content also addresses awareness of the need for operations security. Security awareness techniques can include, for example, displaying posters, offering supplies inscribed with security reminders, generating email advisories/notices from senior organizational officials, displaying logon screen messages, and conducting information security awareness events. Related controls: AT-3, AT-4, PL-4.
Control Number	AT-3
Title	Role-Based Security Training
DHCS Requirement	The organization must provide role-based security training to personnel with assigned security roles and responsibilities: a. Before authorizing access to the information system or performing assigned duties; b. When required by information system changes; and c. With organization-defined frequency thereafter.
Supplemental Guidance (from NIST 800-53)	Organizations determine the appropriate content of security training based on the assigned roles and responsibilities of individuals and the specific security requirements of organizations and the information systems to which personnel have authorized access. In addition, organizations
	provide enterprise architects, information system developers, software developers, acquisition/procurement officials, information system managers, system/network administrators, personnel conducting configuration management and auditing activities, personnel performing independent verification and validation activities, security control assessors, and other personnel having access to system-level software, adequate security-related technical training specifically tailored for their assigned duties. Comprehensive role-based training addresses management, operational, and technical roles and responsibilities covering physical, personnel, and technical safeguards and countermeasures. Such training can include for example, policies, procedures, tools, and artifacts for the organizational security roles defined. Organizations also provide the training necessary for individuals to carry out their responsibilities related to operations and supply chain security within the context of organizational information security programs. Role-based security training also applies to contractors providing services to federal agencies. Related controls: AT-2, AT-4, PL-4, PS-7, SA-3, SA-12, SA-16.
Control Number	AT-4
Title	Security Training Records
DHCS Requirement	The organization must: a. Document and monitor individual information system security training activities including basic security awareness training and specific information system security training; and b. Retain individual training records for 5 years. SSA also requires the organization to certify that each employee, contractor, and agent who views SSA data certify that they understand the potential criminal, civil, and administrative sanctions or penalties for unlawful assess and/or disclosure.
Supplemental Guidance (from NIST 800-53)	Documentation for specialized training may be maintained by individual supervisors at the option of the organization. Related controls: AT-2, AT-3, PM-14.

5. **Contingency Planning (CP)**

Control Number	CP-2
Title	Contingency Plan
DHCS Requirement	The organization must: a. Develop a contingency plan for the information system that: 1. Identifies essential missions and business functions and associated contingency requirements; 2. Provides recovery objectives, restoration priorities, and metrics; 3. Addresses contingency roles, responsibilities, assigned individuals with contact information; 4. Addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure; 5. Addresses eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented; and 6. Is reviewed and approved by a senior manager; b. Distribute copies of the contingency plan to personnel and organizations supporting the contingency plan actions; c. Coordinate contingency planning activities with incident handling activities; d. Review the contingency plan for the information system at least annually; e. Update the contingency plan to address changes to the organization, information system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing; f. Communicate contingency plan changes to personnel and organizations supporting the contingency plan actions; g. Incorporate lessons learned from contingency plan testing, training, or actual contingency activities into contingency testing and training; and h. Protect the contingency plan from unauthorized disclosure and modification.
Supplemental Guidance (from NIST 800-53)	Contingency planning for information systems is part of an overall organizational program for achieving continuity of operations for mission/business functions. Contingency planning addresses both information system restoration and implementation of alternative mission/business processes when systems are compromised. The effectiveness of contingency planning is maximized by considering such planning throughout the phases of the system development life cycle. Performing contingency planning on hardware, software, and firmware development can be an effective means of achieving information system resiliency. Contingency plans reflect the degree of restoration required for organizational information systems since not all systems may need to fully recover to achieve the level of continuity of operations desired. Information system recovery objectives reflect applicable laws, Executive Orders, directives, policies, standards, regulations, and guidelines. In addition to information system availability, contingency plans also address other security-related events resulting in a reduction in mission and/or business effectiveness, such as malicious attacks compromising the confidentiality or integrity of information systems. Actions addressed in contingency plans include, for example, orderly/graceful degradation, information system shutdown, fallback to a manual mode, alternate information flows, and operating in modes reserved for when systems are under attack. By closely coordinating contingency planning with incident handling activities, organizations can ensure that the necessary contingency planning activities are in place and activated in the event of a security incident. Related controls: AC-14, CP-6, CP-7, CP-8, CP-9, CP-10, IR-4, IR-8, MP-2, MP-4, MP-5, PM-8, PM-11.

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

Control Number	DM-2
Title	Data Retention and Disposal
DHCS Requirement	The organization must: a. Retain each collection of Medi-Cal PII no longer than required for the organization's business process or evidentiary purposes; b. Dispose of, destroys, erases, and/or anonymizes the Medi-Cal PII, regardless of the method of storage, in accordance with a NARA-approved record retention schedule and in a manner that prevents loss, theft, misuse, or unauthorized access; and c. Use organization-defined techniques or methods to ensure secure deletion or destruction of PII (including originals, copies, and archived records). .
Supplemental Guidance (from NIST 800-53)	NARA provides retention schedules that govern the disposition of federal records. Program officials coordinate with records officers and with NARA to identify appropriate retention periods and disposal methods. NARA may require organizations to retain PII longer than is operationally needed. In those situations, organizations describe such requirements in the notice. Methods of storage include, for example, electronic, optical media, or paper. Examples of ways organizations may reduce holdings include reducing the types of PII held (e.g., delete Social Security numbers if their use is no longer needed) or shortening the retention period for PII that is maintained if it is no longer necessary to keep PII for long periods of time (this effort is undertaken in consultation with an organization's records officer to receive NARA approval). In both examples, organizations provide notice (e.g., an updated System of Records Notice) to inform the public of any changes in holdings of PII. Certain read-only archiving techniques, such as DVDs, CDs, microfilm, or microfiche, may not permit the removal of individual records without the destruction of the entire database contained on such media. Related controls: AR-4, AU-11, DM-1, MP-1, MP-2, MP-3, MP-4, MP-5, MP-6, MP-7, MP-8, SI-12, TR-1.

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

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

Control Number	IA-5
Title	Authenticator Management
DHCS Requirement	The organization must manage information system authenticators by: a. Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, or device receiving the authenticator; b. Establishing initial authenticator content for authenticators defined by the organization; c. Ensuring that authenticators have sufficient strength of mechanism for their intended use; d. Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators; e. Changing default content of authenticators prior to information system installation; f. Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators; g. Changing/refreshing authenticators within organization-defined time period; h. Protecting authenticator content from unauthorized disclosure and modification; i. Requiring individuals to take, and having devices implement, specific security safeguards to protect authenticators; and j. Changing authenticators for group/role accounts when membership to those accounts changes.
Supplemental Guidance (from NIST 800-53)	Individual authenticators include, for example, passwords, tokens, biometrics, PKI certificates, and key cards. Initial authenticator content is the actual content (e.g., the initial password) as opposed to requirements about authenticator content (e.g., minimum password length). In many cases, developers ship information system components with factory default authentication credentials to allow for initial installation and configuration. Default authentication credentials are often well known, easily discoverable, and present a significant security risk. The requirement to protect individual authenticators may be implemented via control PL-4 or PS-6 for authenticators in the possession of individuals and by controls AC-3, AC-6, and SC-28 for authenticators stored within organizational information systems (e.g., passwords stored in hashed or encrypted formats, files containing encrypted or hashed passwords accessible with administrator privileges). Information systems support individual authenticator management by organization-defined settings and restrictions for various authenticator characteristics including, for example, minimum password length, password composition, validation time window for time synchronous one-time tokens, and number of allowed rejections during the verification stage of biometric authentication. Specific actions that can be taken to safeguard authenticators include, for example, maintaining possession of individual authenticators, not loaning or sharing individual authenticators with others, and reporting lost, stolen, or compromised authenticators immediately. Authenticator management includes issuing and revoking, when no longer needed, authenticators for temporary access such as that required for remote maintenance. Device authenticators include, for example, certificates and passwords. Related controls: AC-2, AC-3, AC-6, CM-6, IA-2, IA-4, IA-8, PL-4, PS- 5, PS-6, SC-12, SC-13, SC-17, SC-28.
Control Number	**IA-5(1)**
Title	Authenticator Management | Password-Based Authentication
DHCS Requirement	The information system, for password-based authentication, must: a. Enforces minimum password complexity of requirements for: * case sensitivity (upper and lower case letters), * number of characters (equal to or greater than fifteen characters), * mix of upper-case letters, lower-case letters, numbers, and special characters (at least one of each type); c. Stores and transmits only cryptographically-protected passwords; d. Enforces password lifetime of at least 180 days; e. Prohibits prior 10 passwords for reuse ; and f. Allows the use of a temporary password for system logons with an immediate change to a permanent password.
Supplemental Guidance (from NIST 800-53)	This control enhancement applies to single-factor authentication of individuals using passwords as individual or group authenticators, and in a similar manner, when passwords are part of multifactor authenticators. This control enhancement does not apply when passwords are used to unlock hardware authenticators (e.g., Personal Identity Verification cards). The implementation of such password mechanisms may not meet all of the requirements in the enhancement. Cryptographically-protected passwords include, for example, encrypted versions of passwords and one-way cryptographic hashes of passwords. The number of changed characters refers to the number of changes required with respect to the total number of positions in the current password. Password lifetime restrictions do not apply to temporary passwords. To mitigate certain brute force attacks against passwords, organizations may also consider salting passwords. Related control: IA-6.

8. **Incident Response (IR)**

Control Number	IR-1
Title	Incident Response Policy and Procedures
DHCS Requirement	The organization must: a. Develops, documents, and disseminates to organization-defined personnel or roles: 1. An incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the incident response policy and associated incident response controls; and b. Reviews and updates the current: 1. Incident response policy with organization-defined frequency; and 2. Incident response procedures with organization-defined frequency. *DHCS and NIST Guidelines encourage agencies to consider establishing incident response teams or identifying individuals specifically responsible for addressing Medi-Cal PII and DHCS data breaches.*
Supplemental Guidance (from NIST 800-53)	This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the IR family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.
Control Number	**IR-2**
Title	Incident Response Training
DHCS Requirement	The organization must provide incident response training to information system users consistent with assigned roles and responsibilities: a. Within organization-defined time period of assuming an incident response role or responsibility; b. When required by information system changes; and c. With organization-defined frequency thereafter.
Supplemental Guidance (from NIST 800-53)	Incident response training provided by organizations is linked to the assigned roles and responsibilities of organizational personnel to ensure the appropriate content and level of detail is included in such training. For example, regular users may only need to know who to call or how to recognize an incident on the information system; system administrators may require additional training on how to handle/remediate incidents; and incident responders may receive more specific training on forensics, reporting, system recovery, and restoration. Incident response training includes user training in the identification and reporting of suspicious activities, both from external and internal sources. Related controls: AT-3, CP-3, IR-8.
Control Number	**IR-4**
Title	Incident Handling
DHCS Requirement	The organization must: a. Implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery; b. Coordinates incident handling activities with contingency planning activities; and c. Incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing, and implements the resulting changes accordingly.
Supplemental Guidance (from NIST 800-53)	Organizations recognize that incident response capability is dependent on the capabilities of organizational information systems and the mission/business processes being supported by those systems. Therefore, organizations consider incident response as part of the definition, design, and development of mission/business processes and information systems. Incident-related information can be obtained from a variety of sources including, for example, audit monitoring, network monitoring, physical access monitoring, user/administrator reports, and reported supply chain events. Effective incident handling capability includes coordination among many organizational entities including, for example, mission/business owners, information system owners, authorizing officials, human resources offices, physical and personnel security offices, legal departments, operations personnel, procurement offices, and the risk executive (function). Related controls: AU-6, CM-6, CP-2, CP-4, IR-2, IR-3, IR-8, PE-6, SC-5, SC-7, SI-3, SI-4, SI-7.

Control Number	IR-8
Title	Incident Response Plan
DHCS Requirement	The organization must: a. Develop an incident response plan that: 1. Provides the organization with a roadmap for implementing its incident response capability; 2. Describes the structure and organization of the incident response capability; 3. Provides a high-level approach for how the incident response capability fits into the overall organization; 4. Meets the unique requirements of te organization, which relate to mission, size, structure, and functions; 5. Defines reportable incidents; 6. Provides metrics for measuring the incident response capability within the organization; 7. Defines the resources and management support needed to effectively maintain and mature an incident response capability; and 8. Is reviewed and approved by organization-defined personnel or roles; b. Distribute copies of the incident response plan to organization-defined incident response personnel (identified by name and/or by role) and organizational elements; c. Review the incident response plan organization-defined frequency; d. Updates the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing; e. Communicate incident response plan changes to organization-defined incident response personnel (identified by name and/or by role) and organizational elements]; and f. Protect the incident response plan from unauthorized disclosure and modification.
Supplemental Guidance (from NIST 800-53)	It is important that organizations develop and implement a coordinated approach to incident response. Organizational missions, business functions, strategies, goals, and objectives for incident response help to determine the structure of incident response capabilities. As part of a comprehensive incident response capability, organizations consider the coordination and sharing of information with external organizations, including, for example, external service providers and organizations involved in the supply chain for organizational information systems. Related controls: MP-2, MP-4, MP-5.

9. **Media Protection (MP)**

Control Number	MP-2
Title	Media Access
DHCS Requirement	The organization must: Restricts access to Medi-Cal PII to County Workers who require access to Medi-Call PII for purposes of administering the Medi-Cal program or as required for the administration of other public benefit programs.
Supplemental Guidance (from NIST 800-53)	Information system media includes both digital and non-digital media. Digital media includes, for example, diskettes, magnetic tapes, external/removable hard disk drives, flash drives, compact disks, and digital video disks. Non-digital media includes, for example, paper and microfilm. Restricting non-digital media access includes, for example, denying access to patient medical records in a community hospital unless the individuals seeking access to such records are authorized healthcare providers. Restricting access to digital media includes, for example, limiting access to design specifications stored on compact disks in the media library to the project leader and the individuals on the development team. Related controls: AC-3, IA-2, MP-4, PE-2, PE-3, PL-2.
Control Number	MP-6
Title	Media Sanitization
DHCS Requirement	The organization must: a. Sanitize media containing Medi-Cal PII prior to disposal, release out of organizational control, or release for reuse in accordance with applicable federal and organizational standards and policies; and b. Employs sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.
Supplemental Guidance (from NIST 800-53)	This control applies to all information system media, both digital and non-digital, subject to disposal or reuse, whether or not the media is considered removable. Examples include media found in scanners, copiers, printers, notebook computers, workstations, network components, and mobile devices. The sanitization process removes information from the media such that the information cannot be retrieved or reconstructed. Sanitization techniques, including clearing, purging, cryptographic erase, and destruction, prevent the disclosure of information to unauthorized individuals when such media is reused or released for disposal. Organizations determine the appropriate sanitization methods recognizing that destruction is sometimes necessary when other methods cannot be applied to media requiring sanitization. Organizations use discretion on the employment of approved sanitization techniques and procedures for media containing information deemed to be in the public domain or publicly releasable, or deemed to have no adverse impact on organizations or individuals if released for reuse or disposal. Sanitization of non-digital media includes, for example, removing a classified appendix from an otherwise unclassified document, or redacting selected sections or words from a document by obscuring the redacted sections/words in a manner equivalent in effectiveness to removing them from the document. NSA standards and policies control the sanitization process for media containing classified information. Related controls: MA-2, MA-4, RA-3, SC-4.

10. **Personnel Security (PS)**

Control Number	PS-3
Title	Personnel Screening
DHCS Requirement	The organization must: a. Screen individuals (employees, contractors and agents) prior to authorizing access to the information system and Medi-Cal PII.
Supplemental Guidance (from NIST 800-53)	Personnel screening and rescreening activities reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, guidance, and specific criteria established for the risk designations of assigned positions. Organizations may define different rescreening conditions and frequencies for personnel accessing information systems based on types of information processed, stored, or transmitted by the systems.
Control Number	PS-4
Title	Personnel Termination
DHCS Requirement	The organization, upon termination of individual employment, must: a. Disable information system access; b. Terminate/revoke any authenticators/credentials associated with the individual; c. Conduct exit interviews, as needed; d. Retrieve all security-related organizational information system-related property; e. Retain access to organizational information and information systems formerly controlled by terminated individual; and f. Notified organization-defined personnel upon termination.
Supplemental Guidance (from NIST 800-53)	Information system-related property includes, for example, hardware authentication tokens, system administration technical manuals, keys, identification cards, and building passes. Exit interviews ensure that terminated individuals understand the security constraints imposed by being former employees and that proper accountability is achieved for information system-related property. Security topics of interest at exit interviews can include, for example, reminding terminated individuals of nondisclosure agreements and potential limitations on future employment. Exit interviews may not be possible for some terminated individuals, for example, in cases related to job abandonment, illnesses, and non-availability of supervisors. Exit interviews are important for individuals with security clearances. Timely execution of termination actions is essential for individuals terminated for cause. In certain situations, organizations consider disabling the information system accounts of individuals that are being terminated prior to the individuals being notified. Related controls: AC-2, IA-4, PE-2, PS-5, PS-6.
Control Number	PS-6
Title	Access Agreements
DHCS Requirement	The organization must: a. Develop and document access agreements for organizational information systems; b. Reviews and updates the access agreements at organization-defined frequency; and c. Ensure that individuals requiring access to organizational information and information systems: 1. Sign appropriate access agreements prior to being granted access; and 2. Re-sign access agreements to maintain access to organizational information systems when access agreements have been updated or at an organization-defined frequency. DHCS requires that contracts for periodic disposal/destruction of case files or other print media contain a non-disclosure agreement signed by all personnel who will encounter products that contain Medi-Cal PII.
Supplemental Guidance (from NIST 800-53)	Supplemental Guidance: Access agreements include, for example, nondisclosure agreements, acceptable use agreements, rules of behavior, and conflict-of-interest agreements. Signed access agreements include an acknowledgement that individuals have read, understand, and agree to abide by the constraints associated with organizational information systems to which access is authorized. Organizations can use electronic signatures to acknowledge access agreements unless specifically prohibited by organizational policy. Related control: PL-4, PS-2, PS-3, PS-4, PS-8.

Control Number	PS-7
Title	Third-Party Personnel Security
DHCS Requirement	The organization must: a. Establishes personnel security requirements including security roles and responsibilities for county agents, subcontractors, and vendors; b. Requires third-party providers to comply with personnel security policies and procedures established by the organization; c. Documents personnel security requirements; d. Requires third-party providers to notify organization-defined personnel or roles of any personnel transfers or terminations of third-party personnel who possess organizational credentials and/or badges, or who have information system privileges within organization-defined time period; and e. Monitors provider compliance. *The service level agreements with the contractors and agents must contain non-disclosure language as it pertains to Medi-Cal PII. The statement shall include, at a minimum, a description of the following:* *1. General Use of Medi-Cal PII;* *2. Security and Privacy Safeguards for Medi-Cal PII;* *3. Unacceptable Use of Medi-Cal PII; and* *4. Enforcement Policies.* *The county department/agency must retain the non-disclosure agreements for at least five (5) to seven (7) years for all contractors and agents who processes, views, or encounters Medi-Cal PII as part of their duties*
Supplemental Guidance (from NIST 800-53)	Third-party providers include, for example, service bureaus, contractors, and other organizations providing information system development, information technology services, outsourced applications, and network and security management. Organizations explicitly include personnel security requirements in acquisition-related documents. Third-party providers may have personnel working at organizational facilities with credentials, badges, or information system privileges issued by organizations. Notifications of third-party personnel changes ensure appropriate termination of privileges and credentials. Organizations define the transfers and terminations deemed reportable by security-related characteristics that include, for example, functions, roles, and nature of credentials/privileges associated with individuals transferred or terminated. Related controls: PS-2, PS-3, PS-4, PS-5, PS-6, SA-9, SA-21.
Control Number	PS-8
Title	Personnel Sanctions
DHCS Requirement	The organization must: a. Employ a formal sanctions process for individuals failing to comply with established information security policies and procedures; and b. Notify organization personnel within the organization-defined time period when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction. *If a member of the county's workforce, as defined at 45 CFR 160.103 and inclusive of an employee, contractor, or agent is subject to an adverse action by the organization (e.g., reduction in pay, disciplinary action, termination of employment, termination of contract for services), DHCS recommends the organization remove his or her access to Medi-Cal PII in advance of the adverse action to reduce the possibility that will the individual will perform unauthorized activities that involve Medi-Cal PII, if applicable.*
Supplemental Guidance (from NIST 800-53)	Organizational sanctions processes reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Sanctions processes are described in access agreements and can be included as part of general personnel policies and procedures for organizations. Organizations consult with the Office of the General Counsel regarding matters of employee sanctions. Related controls: PL-4, PS-6.

11. Physical and Environmental Protection (PE)

Control Number	PE-3
Title	Physical Access Control
DHCS Requirement	The organization must: a. Enforce physical access authorizations at entry and exit points to the facility where the information system resides by; 1. Verifying individual access authorizations before granting access to the facility; and 2. Controlling ingress/egress to the facility using physical access control systems/devices and/or guards; b. Maintain physical access audit logs for entry and exit points; c. Provide security safeguards to control access to areas within the facility officially designated as publicly accessible; d. Escort visitors and monitors visitor activity; e. Secure keys, combinations, and other physical access devices; f. Inventory physical access devices; and g. Changes combinations and keys at minimum when keys are lost, combinations are compromised, or individuals are transferred or terminated
Supplemental Guidance (from NIST 800-53)	This control applies to organizational employees and visitors. Individuals (e.g., employees, contractors, and others) with permanent physical access authorization credentials are not considered visitors. Organizations determine the types of facility guards needed including, for example, professional physical security staff or other personnel such as administrative staff or information system users. Physical access devices include, for example, keys, locks, combinations, and card readers. Safeguards for publicly accessible areas within organizational facilities include, for example, cameras, monitoring by guards, and isolating selected information systems and/or system components in secured areas. Physical access control systems comply with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. The Federal Identity, Credential, and Access Management Program provides implementation guidance for identity, credential, and access management capabilities for physical access control systems. Organizations have flexibility in the types of audit logs employed. Audit logs can be procedural (e.g., a written log of individuals accessing the facility and when such access occurred), automated (e.g., capturing ID provided by a PIV card), or some combination thereof. Physical access points can include facility access points, interior access points to information systems and/or components requiring supplemental access controls, or both. Components of organizational information systems (e.g., workstations, terminals) may be located in areas designated as publicly accessible with organizations safeguarding access to such devices. Related controls: AU-2, AU-6, MP-2, MP-4, PE-2, PE-4, PE-5, PS-3, RA-3.
Control Number	PE-6
Title	Monitoring Physical Access
DHCS Requirement	The organization must: a. Monitors physical access to the facility where the information system resides to detect and respond to physical security incidents; b. Reviews physical access logs organization-defined frequency and upon occurrence of security incidents; and c. Coordinates results of reviews and investigations with the organizational incident response capability.
Supplemental Guidance (from NIST 800-53)	Organizational incident response capabilities include investigations of and responses to detected physical security incidents. Security incidents include, for example, apparent security violations or suspicious physical access activities. Suspicious physical access activities include, for example: (i) accesses outside of normal work hours; (ii) repeated accesses to areas not normally accessed; (iii) accesses for unusual lengths of time; and (iv) out-of-sequence accesses. Related controls: CA-7, IR-4, IR-8.

12. Planning (PL)

Control Number	PL-1
Title	Security Planning Policy and Procedures
DHCS Requirement	The organization must: a. Develop, document, and disseminate to personnel and organizations with access to Medi-Cal PII: 1. A security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the security planning policy and associated security planning controls; and b. Reviews and updates the current: 1. Security planning policy; and 2. Security planning procedures.
Supplemental Guidance (from NIST 800-53)	This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the PL family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.
Control Number	PL-2
Title	System Security Plan
DHCS Requirement	The organization must: a. Develop a security plan for the information system that: 1. Is consistent with the organization's enterprise architecture; 2. Explicitly defines the authorization boundary for the system; 3. Describes the operational context of the information system in terms of missions and business processes; 4. Provides the security categorization of the information system including supporting rationale; 5. Describes the operational environment for the information system and relationships with or connections to other information systems; 6. Provides an overview of the security requirements for the system; 7. Identifies any relevant overlays, if applicable; 8. Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring decisions; and 9. Is reviewed and approved by the authorizing official or designated representative prior to plan implementation; b. Distribute copies of the security plan and communicates subsequent changes to the plan to personnel and organizations with security responsibilities; c. Review the security plan for the information system; d. Update the plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments; and e. Protect the security plan from unauthorized disclosure and modification. *Organization's security plan should include detailed information specific to safeguarding Medi-Cal PII.*
Supplemental Guidance (from NIST 800-53)	Security plans relate security requirements to a set of security controls and control enhancements. Security plans also describe, at a high level, how the security controls and control enhancements meet those security requirements, but do not provide detailed, technical descriptions of the specific design or implementation of the controls/enhancements. Security plans contain sufficient information (including the specification of parameter values for assignment and selection statements either explicitly or by reference) to enable a design and implementation that is unambiguously compliant with the intent of the plans and subsequent determinations of risk to organizational operations and assets, individuals, other organizations, and the Nation if the plan is implemented as intended. Organizations can also apply tailoring guidance to the security control baselines in Appendix D and CNSS Instruction 1253 to develop overlays for community-wide use or to address specialized requirements, technologies, or missions/environments of operation (e.g., DoD-tactical, Federal Public Key Infrastructure, or Federal Identity, Credential, and Access Management, space operations). Appendix I provides guidance on developing overlays. Security plans need not be single documents; the plans can be a collection of various documents including documents that already exist. Effective security plans make extensive use of references to policies, procedures, and additional documents (e.g., design and implementation specifications) where more detailed information can be obtained. This reduces the documentation requirements associated with security programs and maintains security-related information in other established management/operational areas related to enterprise architecture, system development life cycle, systems engineering, and acquisition. For example, security plans do not contain detailed contingency plan or incident response plan information but instead provide explicitly or by reference, sufficient information to define what needs to be accomplished by those plans. Related controls: AC-2, AC-6, AC-14, AC-17, AC-20, CA-2, CA-3, CA-7, CM-9, CP-2, IR-8, MA-4, MA-5, MP-2, MP-4, MP-5, PL-7, PM-1, PM-7, PM-8, PM-9, PM-11, SA-5, SA-17.

13. Risk Assessment (RA)

Control Number	RA-1
Title	Risk Assessment Policy and Procedures
DHCS Requirement	The organization must: a. Develop, document, and disseminate to system owners using Medi-Cal PII: 1. A risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls.
Supplemental Guidance (from NIST 800-53)	This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the RA family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.
Control Number	RA-3
Title	Risk Assessment
DHCS Requirement	The organization must: a. Conduct an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits; b. Documents risk assessment results in a risk assessment report or organization defined risk report document. c. Review risk assessment results annually; and e. Update the risk assessment whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system.
Supplemental Guidance (from NIST 800-53)	Clearly defined authorization boundaries are a prerequisite for effective risk assessments. Risk assessments take into account threats, vulnerabilities, likelihood, and impact to organizational operations and assets, individuals, other organizations, and the Nation based on the operation and use of information systems. Risk assessments also take into account risk from external parties (e.g., service providers, contractors operating information systems on behalf of the organization, individuals accessing organizational information systems, outsourcing entities). In accordance with OMB policy and related E-authentication initiatives, authentication of public users accessing federal information systems may also be required to protect nonpublic or privacy-related information. As such, organizational assessments of risk also address public access to federal information systems. Risk assessments (either formal or informal) can be conducted at all three tiers in the risk management hierarchy (i.e., organization level, mission/business process level, or information system level) and at any phase in the system development life cycle. Risk assessments can also be conducted at various steps in the Risk Management Framework, including categorization, security control selection, security control implementation, security control assessment, information system authorization, and security control monitoring. RA-3 is noteworthy in that the control must be partially implemented prior to the implementation of other controls in order to complete the first two steps in the Risk Management Framework. Risk assessments can play an important role in security control selection processes, particularly during the application of tailoring guidance, which includes security control supplementation. Related controls: RA-2, PM- 9.

Control Number	RA-5
Title	Vulnerability Scanning
DHCS Requirement	The organization must: a. Scan for vulnerabilities in the information system and hosted applications at a minimum of a monthly basis and when new vulnerabilities potentially affecting the system/applications are identified and reported; b. Employ vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for: 1. Enumerating platforms, software flaws, and improper configurations; a. Analyze vulnerability scan reports and results from security control assessments; b. Remediate legitimate vulnerabilities within organization defined time periods in accordance with an organizational assessment of risk; and c. Share information obtained from the vulnerability scanning process and security control assessments with all impacted system owners to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).
Supplemental Guidance (from NIST 800-53)	Security categorization of information systems guides the frequency and comprehensiveness of vulnerability scans. Organizations determine the required vulnerability scanning for all information system components, ensuring that potential sources of vulnerabilities such as networked printers, scanners, and copiers are not overlooked. Vulnerability analyses for custom software applications may require additional approaches such as static analysis, dynamic analysis, binary analysis, or a hybrid of the three approaches. Organizations can employ these analysis approaches in a variety of tools (e.g., web-based application scanners, static analysis tools, binary analyzers) and in source code reviews. Vulnerability scanning includes, for example: (i) scanning for patch levels; (ii) scanning for functions, ports, protocols, and services that should not be accessible to users or devices; and (iii) scanning for improperly configured or incorrectly operating information flow control mechanisms. Organizations consider using tools that express vulnerabilities in the Common Vulnerabilities and Exposures (CVE) naming convention and that use the Open Vulnerability Assessment Language (OVAL) to determine/test for the presence of vulnerabilities. Suggested sources for vulnerability information include the Common Weakness Enumeration (CWE) listing and the National Vulnerability Database (NVD). In addition, security control assessments such as red team exercises provide other sources of potential vulnerabilities for which to scan. Organizations also consider using tools that express vulnerability impact by the Common Vulnerability Scoring System (CVSS). Related controls: CA-2, CA-7, CM-4, CM-6, RA-2, RA-3, SA-11, SI-2.

14. Security Assessment and Authorization (CA)

Control Number	CA-2
Title	Security Assessments
DHCS Requirement	The organization must: a. Develops a security assessment plan that describes the scope of the assessment including: 1. Security controls and control enhancements under assessment; 2. Assessment procedures to be used to determine security control effectiveness; and 3. Assessment environment, assessment team, and assessment roles and responsibilities; b. Assesses the security controls in the information system and its environment of operation with organization-defined frequency to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security requirements; c. Produces a security assessment report that documents the results of the assessment; and d. Provides the results of the security control assessment to organization-defined individuals or roles.
Supplemental Guidance (from NIST 800-53)	Organizations assess security controls in organizational information systems and the environments in which those systems operate as part of: (i) initial and ongoing security authorizations; (ii) FISMA annual assessments; (iii) continuous monitoring; and (iv) system development life cycle activities. Security assessments: (i) ensure that information security is built into organizational information systems; (ii) identify weaknesses and deficiencies early in the development process; (iii) provide essential information needed to make risk-based decisions as part of security authorization processes; and (iv) ensure compliance to vulnerability mitigation procedures. Assessments are conducted on the implemented security controls from Appendix F (main catalog) and Appendix G (Program Management controls) as documented in System Security Plans and Information Security Program Plans. Organizations can use other types of assessment activities such as vulnerability scanning and system monitoring to maintain the security posture of information systems during the entire life cycle. Security assessment reports document assessment results in sufficient detail as deemed necessary by organizations, to determine the accuracy and completeness of the reports and whether the security controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting security requirements. The FISMA requirement for assessing security controls at least annually does not require additional assessment activities to those activities already in place in organizational security authorization processes. Security assessment results are provided to the individuals or roles appropriate for the types of assessments being conducted. For example, assessments conducted in support of security authorization decisions are provided to authorizing officials or authorizing official designated representatives. To satisfy annual assessment requirements, organizations can use assessment results from the following sources: (i) initial or ongoing information system authorizations; (ii) continuous monitoring; or (iii) system development life cycle activities. Organizations ensure that security assessment results are current, relevant to the determination of security control effectiveness, and obtained with the appropriate level of assessor independence. Existing security control assessment results can be reused to the extent that the results are still valid and can also be supplemented with additional assessments as needed. Subsequent to initial authorizations and in accordance with OMB policy, organizations assess security controls during continuous monitoring. Organizations establish the frequency for ongoing security control assessments in accordance with organizational continuous monitoring strategies. Information Assurance Vulnerability Alerts provide useful examples of vulnerability mitigation procedures. External audits (e.g., audits by external entities such as regulatory agencies) are outside the scope of this control. Related controls: CA-5, CA-6, CA-7, PM-9, RA-5, SA-11, SA-12, SI-4.

Control Number	CA-3
Title	System Interconnections
DHCS Requirement	The organization must: a. Authorizes connections from the information system to other information systems through the use of Interconnection Security Agreements; b. Documents, for each interconnection, the interface characteristics, security requirements, and the nature of the information communicated; and c. Reviews and updates Interconnection Security Agreements [Assignment: organization-defined frequency].
Supplemental Guidance (from NIST 800-53)	This control applies to dedicated connections between information systems (i.e., system interconnections) and does not apply to transitory, user-controlled connections such as email and website browsing. Organizations carefully consider the risks that may be introduced when information systems are connected to other systems with different security requirements and security controls, both within organizations and external to organizations. Authorizing officials determine the risk associated with information system connections and the appropriate controls employed. If interconnecting systems have the same authorizing official, organizations do not need to develop Interconnection Security Agreements. Instead, organizations can describe the interface characteristics between those interconnecting systems in their respective security plans. If interconnecting systems have different authorizing officials within the same organization, organizations can either develop Interconnection Security Agreements or describe the interface characteristics between systems in the security plans for the respective systems. Organizations may also incorporate Interconnection Security Agreement information into formal contracts, especially for interconnections established between federal agencies and nonfederal (i.e., private sector) organizations. Risk considerations also include information systems sharing the same networks. For certain technologies (e.g., space, unmanned aerial vehicles, and medical devices), there may be specialized connections in place during preoperational testing. Such connections may require Interconnection Security Agreements and be subject to additional security controls. Related controls: AC-3, AC-4, AC-20, AU-2, AU-12, AU-16, CA-7, IA-3, SA-9, SC-7, SI-4.
Control Number	CA-7
Title	Continuous Monitoring
DHCS Requirement	The organization must develop a continuous monitoring strategy and implement a continuous monitoring program that includes: a. Establishment of Medi-Cal PII security controls to be monitored; c. Ongoing security control assessments in accordance with the organizational continuous monitoring strategy; d. Ongoing security status monitoring of Medi-Cal PII security controls in accordance with the organizational continuous monitoring strategy; e. Correlation and analysis of security-related information generated by assessments and monitoring; f. Response actions to address results of the analysis of security-related information; and g. Reporting the security status of organization and the information system to organization-defined personnel or roles and to DHCS when requested.
Supplemental Guidance (from NIST 800-53)	Continuous monitoring programs facilitate ongoing awareness of threats, vulnerabilities, and information security to support organizational risk management decisions. The terms continuous and ongoing imply that organizations assess/analyze security controls and information security-related risks at a frequency sufficient to support organizational risk-based decisions. The results of continuous monitoring programs generate appropriate risk response actions by organizations. Continuous monitoring programs also allow organizations to maintain the security authorizations of information systems and common controls over time in highly dynamic environments of operation with changing mission/business needs, threats, vulnerabilities, and technologies. Having access to security-related information on a continuing basis through reports/dashboards gives organizational officials the capability to make more effective and timely risk management decisions, including ongoing security authorization decisions. Automation supports more frequent updates to security authorization packages, hardware/software/firmware inventories, and other system information. Effectiveness is further enhanced when continuous monitoring outputs are formatted to provide information that is specific, measurable, actionable, relevant, and timely. Continuous monitoring activities are scaled in accordance with the security categories of information systems. Related controls: CA-2, CA-5, CA-6, CM-3, CM-4, PM-6, PM-9, RA-5, SA-11, SA-12, SI-2, SI-4.

Control Number	CA-8
Title	Penetration Testing
DHCS Requirement	The organization must conduct penetration testing annually on systems storing, processing, or transmitting Medi-Cal PII.
Supplemental Guidance (from NIST 800-53)	Penetration testing is a specialized type of assessment conducted on information systems or individual system components to identify vulnerabilities that could be exploited by adversaries. Such testing can be used to either validate vulnerabilities or determine the degree of resistance organizational information systems have to adversaries within a set of specified constraints (e.g., time, resources, and/or skills). Penetration testing attempts to duplicate the actions of adversaries in carrying out hostile cyber-attacks against organizations and provides a more in-depth analysis of security-related weaknesses/deficiencies. Organizations can also use the results of vulnerability analyses to support penetration testing activities. Penetration testing can be conducted on the hardware, software, or firmware components of an information system and can exercise both physical and technical security controls. A standard method for penetration testing includes, for example: (i) pretest analysis based on full knowledge of the target system; (ii) pretest identification of potential vulnerabilities based on pretest analysis; and (iii) testing designed to determine exploitability of identified vulnerabilities. All parties agree to the rules of engagement before the commencement of penetration testing scenarios. Organizations correlate the penetration testing rules of engagement with the tools, techniques, and procedures that are anticipated to be employed by adversaries carrying out attacks. Organizational risk assessments guide decisions on the level of independence required for personnel conducting penetration testing. Related control: SA-12.

15. System and Communications Protection (SC)

Control Number	SC-7
Title	Boundary Protection
DHCS Requirement	The organization information system must: a. Monitor and control communications at the external boundary of the system and at key internal boundaries within the system; b. Implements subnetworks for publicly accessible system components that are physically and logically separated from internal organizational networks; and c. Connect to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.
Supplemental Guidance (from NIST 800-53)	Managed interfaces include, for example, gateways, routers, firewalls, guards, network-based malicious code analysis and virtualization systems, or encrypted tunnels implemented within a security architecture (e.g., routers protecting firewalls or application gateways residing on protected subnetworks). Subnetworks that are physically or logically separated from internal networks are referred to as demilitarized zones or DMZs. Restricting or prohibiting interfaces within organizational information systems includes, for example, restricting external web traffic to designated web servers within managed interfaces and prohibiting external traffic that appears to be spoofing internal addresses. Organizations consider the shared nature of commercial telecommunications services in the implementation of security controls associated with the use of such services. Commercial telecommunications services are commonly based on network components and consolidated management systems shared by all attached commercial customers, and may also include third party-provided access lines and other service elements. Such transmission services may represent sources of increased risk despite contract security provisions. Related controls: AC-4, AC-17, CA-3, CM-7, CP-8, IR-4, RA-3, SC-5, SC-13.
Control Number	SC-8
Title	Transmission Confidentiality and Integrity
DHCS Requirement	The organization information system must: Protect the confidentiality of transmitted information.
Supplemental Guidance (from NIST 800-53)	This control applies to both internal and external networks and all types of information system components from which information can be transmitted (e.g., servers, mobile devices, notebook computers, printers, copiers, scanners, facsimile machines). Communication paths outside the physical protection of a controlled boundary are exposed to the possibility of interception and modification. Protecting the confidentiality and/or integrity of organizational information can be accomplished by physical means (e.g., by employing protected distribution systems) or by logical means (e.g., employing encryption techniques). Organizations relying on commercial providers offering transmission services as commodity services rather than as fully dedicated services (i.e., services which can be highly specialized to individual customer needs), may find it difficult to obtain the necessary assurances regarding the implementation of needed security controls for transmission confidentiality/integrity. In such situations, organizations determine what types of confidentiality/integrity services are available in standard, commercial telecommunication service packages. If it is infeasible or impractical to obtain the necessary security controls and assurances of control effectiveness through appropriate contracting vehicles, organizations implement appropriate compensating security controls or explicitly accept the additional risk. Related controls: AC-17, PE-4.

Control Number	SC-8(1)
Title	Transmission Confidentiality and Integrity | Cryptographic or Alternate Physical Protection
DHCS Requirement	The organization information system must implement cryptographic mechanisms to prevent unauthorized disclosure of information during transmission.
Supplemental Guidance (from NIST 800-53)	Encrypting information for transmission protects information from unauthorized disclosure and modification. Cryptographic mechanisms implemented to protect information integrity include, for example, cryptographic hash functions which have common application in digital signatures, checksums, and message authentication codes. Alternative physical security safeguards include, for example, protected distribution systems. Related control: SC-13.
Control Number	SC-13
Title	Cryptographic Protection
DHCS Requirement	The organization information system must implement FIPS 140-3 compliant encryption modules in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.
Supplemental Guidance (from NIST 800-53)	Cryptography can be employed to support a variety of security solutions including, for example, the protection of classified and Controlled Unclassified Information, the provision of digital signatures, and the enforcement of information separation when authorized individuals have the necessary clearances for such information but lack the necessary formal access approvals. Cryptography can also be used to support random number generation and hash generation. Generally applicable cryptographic standards include FIPS-validated cryptography and NSA-approved cryptography. This control does not impose any requirements on organizations to use cryptography. However, if cryptography is required based on the selection of other security controls, organizations define each type of cryptographic use and the type of cryptography required (e.g., protection of classified information: NSA-approved cryptography; provision of digital signatures: FIPS-validated cryptography). Related controls: AC-2, AC-3, AC-7, AC-17, AC-18, AU-9, AU-10, CM-11, CP-9, IA-3, IA-7, MA-4, MP-2, MP-4, MP-5, SA-4, SC-8, SC-12, SC-28, SI-7.
Control Number	SC-28
Title	Protection of Information at Rest
DHCS Requirement	The organization information system must: Protect the confidentiality of Medi-Cal PII at rest.
Supplemental Guidance (from NIST 800-53)	This control addresses the confidentiality and integrity of information at rest and covers user information and system information. Information at rest refers to the state of information when it is located on storage devices as specific components of information systems. System-related information requiring protection includes, for example, configurations or rule sets for firewalls, gateways, intrusion detection/prevention systems, filtering routers, and authenticator content. Organizations may employ different mechanisms to achieve confidentiality and integrity protections, including the use of cryptographic mechanisms and file share scanning. Integrity protection can be achieved, for example, by implementing Write-Once-Read-Many (WORM) technologies. Organizations may also employ other security controls including, for example, secure off-line storage in lieu of online storage when adequate protection of information at rest cannot otherwise be achieved and/or continuous monitoring to identify malicious code at rest. Related controls: AC-3, AC-6, CA-7, CM-3, CM-5, CM-6, PE-3, SC-8, SC-13, SI-3, SI-7.

16. System and Information Integrity (SI)

Control Number	SI-2
Title	Flaw Remediation
DHCS Requirement	The organization must: a. Identify, report, and correct information system flaws; b. Tests software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation; c. Installs security-relevant software and firmware updates, within acceptable organization standards, of the release of the updates; and d. Incorporates flaw remediation into the organizational configuration management process.
Supplemental Guidance (from NIST 800-53)	Organizations identify information systems affected by announced software flaws including potential vulnerabilities resulting from those flaws, and report this information to designated organizational personnel with information security responsibilities. Security-relevant software updates include, for example, patches, service packs, hot fixes, and anti-virus signatures. Organizations also address flaws discovered during security assessments, continuous monitoring, incident response activities, and system error handling. Organizations take advantage of available resources such as the Common Weakness Enumeration (CWE) or Common Vulnerabilities and Exposures (CVE) databases in remediating flaws discovered in organizational information systems. By incorporating flaw remediation into ongoing configuration management processes, required/anticipated remediation actions can be tracked and verified. Flaw remediation actions that can be tracked and verified include, for example, determining whether organizations follow US-CERT guidance and Information Assurance Vulnerability Alerts. Organization-defined time periods for updating security-relevant software and firmware may vary based on a variety of factors including, for example, the security category of the information system or the criticality of the update (i.e., severity of the vulnerability related to the discovered flaw). Some types of flaw remediation may require more testing than other types. Organizations determine the degree and type of testing needed for the specific type of flaw remediation activity under consideration and also the types of changes that are to be configuration-managed. In some situations, organizations may determine that the testing of software and/or firmware updates is not necessary or practical, for example, when implementing simple anti-virus signature updates. Organizations may also consider in testing decisions, whether security-relevant software or firmware updates are obtained from authorized sources with appropriate digital signatures. Related controls: CA-2, CA-7, CM-3, CM-5, CM-8, MA-2, IR-4, RA-5, SA-10, SA-11, SI-11.
Control Number	SI-3
Title	Malicious Code Protection
DHCS Requirement	The organization must: a. Employ malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code; b. Update malicious code protection mechanisms whenever new releases are available in accordance with organizational configuration management policy and procedures; c. Configure malicious code protection mechanisms to: 1. Perform periodic scans of the information system and real-time scans of files from external sources at the endpoint and network entry/exit points as the files are downloaded, opened, or executed in accordance with organizational security policy; and 2. Block malicious code or quarantine malicious code, and send alert to administrator for incident handling in response to malicious code detection; and d. Address the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system
Supplemental Guidance (from NIST 800-53)	Information system entry and exit points include, for example, firewalls, electronic mail servers, web servers, proxy servers, remote-access servers, workstations, notebook computers, and mobile devices. Malicious code includes, for example, viruses, worms, Trojan horses, and spyware. Malicious code can also be encoded in various formats (e.g., UUENCODE, Unicode), contained within compressed or hidden files, or hidden in files using steganography. Malicious code can be transported by different means including, for example, web accesses, electronic mail, electronic mail attachments, and portable storage devices. Malicious code insertions occur through the exploitation of information system vulnerabilities. Malicious code protection mechanisms include, for example, anti-virus signature definitions and reputation-based technologies. A variety of technologies and methods exist to limit or eliminate the effects of malicious code. Pervasive configuration management and comprehensive software integrity controls may be effective in preventing execution of unauthorized code. In addition to commercial off-the-shelf software, malicious code may also be present in custom-built software. This could include, for example, logic bombs, back doors, and other types of cyber attacks that could affect organizational missions/business functions. Traditional malicious code protection mechanisms cannot always detect such code. In these situations, organizations rely instead on other safeguards including, for example, secure coding practices, configuration management and control, trusted procurement processes, and monitoring practices to help ensure that software does not perform functions other than the functions intended. Organizations may determine that in response to the detection of malicious code, different actions may be warranted. For example, organizations can define actions in response to malicious code detection during periodic scans, actions in response to detection of malicious downloads, and/or actions in response to detection of maliciousness when attempting to open or execute files. Related controls: CM-3, MP-2, SA-4, SA-8, SA-12, SA-13, SC-7, SC-26, SC-44, SI-2, SI-4, SI-7.

Control Number	SI-4
Title	Information System Monitoring
DHCS Requirement	The organization must: a. Monitor the information system to detect: 1. Attacks and indicators of potential attacks in accordance with organization-defined monitoring objectives; and 2. Unauthorized local, network, and remote connections; b. Identify unauthorized use of the information system through organization-defined techniques and methods; c. Deploy monitoring devices: 1. Strategically within the information system to collect organization-determined essential information; and 2. At ad hoc locations within the system to track specific types of transactions of interest to the organization; d. Protect information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion; e. Heighten the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations and assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information; Relevant risk would apply to anything impacting the confidentiality integrity or availability of the information system. f. Obtain legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations; and g. Provides organization-defined information system monitoring information to organization-defined personnel and DHCS as needed.
Supplemental Guidance (from NIST 800-53)	Information system monitoring includes external and internal monitoring. External monitoring includes the observation of events occurring at the information system boundary (i.e., part of perimeter defense and boundary protection). Internal monitoring includes the observation of events occurring within the information system. Organizations can monitor information systems, for example, by observing audit activities in real time or by observing other system aspects such as access patterns, characteristics of access, and other actions. The monitoring objectives may guide determination of the events. Information system monitoring capability is achieved through a variety of tools and techniques (e.g., intrusion detection systems, intrusion prevention systems, malicious code protection software, scanning tools, audit record monitoring software, network monitoring software). Strategic locations for monitoring devices include, for example, selected perimeter locations and near server farms supporting critical applications, with such devices typically being employed at the managed interfaces associated with controls SC-7 and AC-17. Einstein network monitoring devices from the Department of Homeland Security can also be included as monitoring devices. The granularity of monitoring information collected is based on organizational monitoring objectives and the capability of information systems to support such objectives. Specific types of transactions of interest include, for example, Hyper Text Transfer Protocol (HTTP) traffic that bypasses HTTP proxies. Information system monitoring is an integral part of organizational continuous monitoring and incident response programs. Output from system monitoring serves as input to continuous monitoring and incident response programs. A network connection is any connection with a device that communicates through a network (e.g., local area network, Internet). A remote connection is any connection with a device communicating through an external network (e.g., the Internet). Local, network, and remote connections can be either wired or wireless. Related controls: AC-3, AC-4, AC-8, AC-17, AU-2, AU-6, AU-7, AU-9, AU-12, CA-7, IR-4, PE-3, RA-5, SC-7, SC-26, SC-35, SI-3, SI-7.

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

17. System and Services Acquisition (SA)

Control Number	SA-9
Title	External Information System Services
DHCS Requirement	The organization must: a. Require that providers of external information system services comply with organizational information security requirements and employ organization-defined security controls in accordance with DHCS PSA, applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance; b. Defines and documents government oversight and user roles and responsibilities with regard to external information system services; and c. Employs organization-defined processes, methods, and techniques to monitor security control compliance by external service providers on an ongoing basis. *The state organization will provide its contractors and agents with copies of the Agreement, related IEAs, and all related attachments before initial disclosure of Medi-Cal PII to such contractors and agents. Prior to signing the Agreement, and thereafter at DHCS's request, the state organization will obtain from its contractors and agents a current list of the employees of such contractors and agents with access to Medi-Cal PII and provide such lists to DHCS.*
Supplemental Guidance (from NIST 800-53)	External information system services are services that are implemented outside of the authorization boundaries of organizational information systems. This includes services that are used by, but not a part of, organizational information systems. FISMA and OMB policy require that organizations using external service providers that are processing, storing, or transmitting federal information or operating information systems on behalf of the federal government ensure that such providers meet the same security requirements that federal agencies are required to meet. Organizations establish relationships with external service providers in a variety of ways including, for example, through joint ventures, business partnerships, contracts, interagency agreements, lines of business arrangements, licensing agreements, and supply chain exchanges. The responsibility for managing risks from the use of external information system services remains with authorizing officials. For services external to organizations, a chain of trust requires that organizations establish and retain a level of confidence that each participating provider in the potentially complex consumer-provider relationship provides adequate protection for the services rendered. The extent and nature of this chain of trust varies based on the relationships between organizations and the external providers. Organizations document the basis for trust relationships so the relationships can be monitored over time. External information system services documentation includes government, service providers, end user security roles and responsibilities, and service-level agreements. Service-level agreements define expectations of performance for security controls, describe measurable outcomes, and identify remedies and response requirements for identified instances of noncompliance. Related controls: CA-3, IR-7, PS-7.

Control Number	SA-11
Title	Developer Security Testing And Evaluation
DHCS Requirement	The organization must require the developer of the information system, system component, or information system service to: a. Create and implement a security assessment plan; b. Perform [Selection (one or more): unit; integration; system; regression] testing/evaluation at [Assignment: organization-defined depth and coverage]; c. Produce evidence of the execution of the security assessment plan and the results of the security testing/evaluation; d. Implement a verifiable flaw remediation process; and e. Correct flaws identified during security testing/evaluation
Supplemental Guidance (from NIST 800-53)	Supplemental Guidance: Developmental security testing/evaluation occurs at all post-design phases of the system development life cycle. Such testing/evaluation confirms that the required security controls are implemented correctly, operating as intended, enforcing the desired security policy, and meeting established security requirements. Security properties of information systems may be affected by the interconnection of system components or changes to those components. These interconnections or changes (e.g., upgrading or replacing applications and operating systems) may adversely affect previously implemented security controls. This control provides additional types of security testing/evaluation that developers can conduct to reduce or eliminate potential flaws. Testing custom software applications may require approaches such as static analysis, dynamic analysis, binary analysis, or a hybrid of the three approaches. Developers can employ these analysis approaches in a variety of tools (e.g., web-based application scanners, static analysis tools, binary analyzers) and in source code reviews. Security assessment plans provide the specific activities that developers plan to carry out including the types of analyses, testing, evaluation, and reviews of software and firmware components, the degree of rigor to be applied, and the types of artifacts produced during those processes. The depth of security testing/evaluation refers to the rigor and level of detail associated with the assessment process (e.g., black box, gray box, or white box testing). The coverage of security testing/evaluation refers to the scope (i.e., number and type) of the artifacts included in the assessment process. Contracts specify the acceptance criteria for security assessment plans, flaw remediation processes, and the evidence that the plans/processes have been diligently applied. Methods for reviewing and protecting assessment plans, evidence, and documentation are commensurate with the security category or classification level of the information system. Contracts may specify documentation protection requirements. Related controls: CA-2, CM-4, SA-3, SA-4, SA-5, SI-2.

B. Minimum Cloud Security Requirements

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

1. Identify and classify assets to focus and prioritize efforts in aligning business needs and risk management.
2. Each information asset for which the County Department/Agency entity has ownership responsibility shall be inventoried and identified to include the following:
    a. Description and value of the information asset.
    b. Owner of the information asset.
    c. Custodians of the information asset.
    d. Users of the information asset.
    e. Classification of information.
    f. FIPS Publication 199 categorization and level of protection (Low, Moderate, or High).
    g. Importance of information assets to the execution of the Agency/state entity's mission and program function.
    h. Potential consequences and impacts if confidentiality, integrity, and availability of the information asset were compromised.

3. Security of cloud services stems from managing authentication and fine-grained authorization. To safeguard cloud systems, County Department/Agency shall establish processes and procedures to ensure:
    a. Maintenance of user identities, including both provisioning and de-provisioning;
    b. Enforcement of password policies or more advanced multifactor mechanisms to authenticate users and devices;
    c. Management of access control rules, limiting access to the minimum necessary to complete defined responsibilities;
    d. Separation of duties to avoid functional conflicts;
    e. Periodic recertification of access control rules to identify those that are no longer needed or provide overly broad clearance;
    f. Use of privileged accounts that can bypass security are restricted and audited;
    g. Systems to administer access based on roles are defined and installed; and
    h. Encryption keys and system security certificates are effectively generated, exchanged, stored and safeguarded.

4. Infrastructure protection controls limit the impact of unintended access or potential vulnerabilities. PaaS and SaaS resources may already have these controls implemented by the service provider. County Department/Agency must configure information assets to provide only

essential capabilities.

5. County Department/Agency are entrusted with protecting the integrity and confidentiality of data processed by their information systems. Cloud technologies simplify data protection by providing managed data storage services with native protection and backup features, but these features must be configured and managed appropriately.
6. Detective controls identify potential security threats or incidents, supporting timely investigation and response. County Department/Agency must continuously identify and remediate vulnerabilities.
7. Response controls enable timely event and incident response which is essential to reducing the impact if an incident were to occur. Compliance with incident management requirements as outlined in VII. Notification and Investigation of Breaches and Security Incidents.
8. Recover controls facilitate long-term recovery activities following events or incidents. With cloud services, primarily SaaS solutions, the services provider hosts the data in its application, and unless properly planned and provisioned for in the contract with the service provider it may be difficult or impossible to obtain the data in a usable format at contract termination. County Department/Agency must ensure agreements with cloud service providers include recover controls.

C. ***Minimum Necessary.*** Only the minimum necessary amount of Medi-Cal PII required to perform required business functions applicable to the terms of this Agreement may be used, disclosed, copied, downloaded, or exported.

D. ***Transmission and Storage of Medi-Cal PII.*** All persons that will be working with Medi-Cal PII shall employ FIPS 140-2 or greater approved security functions as described in section 6.2.2 of NIST SP 800-140Cr1 encryption of Medi-Cal PII at rest and in motion unless County Department/Agency determines it is not reasonable and appropriate to do so based upon a risk assessment, and equivalent alternative measures are in place and documented as such. In addition, County Department/Agency shall maintain, at a minimum, the most current industry standards for transmission and storage of DHCS data and other confidential information.

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

If DHCS changes the terms of the DHCS Remote to Work Policy, DHCS will, as soon as reasonably possible, supply copies to CWDA and the County Department/Agency or its designee as well as DHCS' proposed target date for compliance. For a period of thirty (30) days, DHCS will accept input from

CWDA and the County Department/Agency or its designee on the proposed changes. DHCS will issue a new policy in a future MEDIL. If the County Department/Agency is unable to comply with these standards, the CWD will be asked to develop a Plan of Action and Milestones (POA&M) detailing a concrete roadmap to becoming fully compliant with the policy's standard. The POA&M must be provided to DHCS for review and approval. Any CWDA who is under a POA&M will be required to provide quarterly updates to DHCS until the fully compliant.

VI. AUDIT CONTROLS

A. ***Audit Control Mechanisms.*** The County Department/Agency shall ensure audit control mechanisms are in place that are compliant with the Technical Security Controls within Section V of this Agreement..

B. ***Anomalies.*** When the County Department/Agency or DHCS suspects MEDS usage anomalies, the County Department/Agency shall work with DHCS to investigate the anomalies and report conclusions of such investigations and remediation to DHCS.

C. ***Notification to DHCS in event County Department/Agency is subject to other Audit.*** If County Department/Agency is the subject of an audit, compliance review, investigation, or any proceeding that is related to the performance of its obligations pursuant to this Agreement, or is the subject of any judicial or administrative proceeding alleging a violation of law related to the privacy and security of PII, including but not limited to Medi-Cal PII, the County Department/Agency shall promptly notify DHCS unless it is legally prohibited from doing so.

VII. PAPER, RECORD, AND MEDIA CONTROLS

A. ***Supervision of Data.*** Medi-Cal PII shall not be left unattended at any time, unless it is locked in a file cabinet, file room, desk or office at the individual's place of employment or at home when working remotely. Unattended means that information may be observed by an individual not authorized to access the information.

B. ***Data in Vehicles.*** The County Department/Agency shall have policies that include, based on applicable risk factors, a description of the circumstances under which the County Workers can transport Medi-Cal PII, as well as the physical security requirements during transport. A County Department/Agency that chooses to permit its County Workers to leave records unattended in vehicles, shall include provisions in its policies to provide that the Medi-Cal PII is stored in a non-visible area such as a trunk, that the vehicle is locked, and that under no circumstances permit Medi-Cal PII to be left unattended in a vehicle overnight or for other extended periods of time.

C. ***Public Modes of Transportation.*** Medi-Cal PII shall not be left unattended at any time in airplanes, buses, trains, etc., inclusive of baggage areas. This should be included in training due to the nature of the risk.

D. ***Escorting Visitors.*** Visitors to areas where Medi-Cal PII is contained shall be escorted, and Medi-Cal PII shall be kept out of sight while visitors are in the area.

E. ***Confidential Destruction.*** Medi-Cal PII shall be disposed of through confidential means, such as cross cut shredding or pulverizing.

F. ***Removal of Data.*** Medi-Cal PII shall not be removed from the premises of County Department/Agency except for justifiable business purposes.

G. ***Faxing.***

1. Faxes containing Medi-Cal PII shall not be left unattended and fax machines shall be in secure areas.

2. Faxes shall contain a confidentiality statement notifying persons receiving faxes in error to destroy them and notify the sender.

3. Fax numbers shall be verified with the intended recipient before sending the fax.

H. ***Mailing.***

1. Mailings containing Medi-Cal PII shall be sealed and secured from damage or inappropriate viewing of PII to the extent possible.

2. Mailings that include 500 or more individually identifiable records containing Medi-Cal PII in a single package shall be sent using a tracked mailing method that includes verification of delivery and receipt.

VIII. NOTIFICATION AND INVESTIGATION OF BREACHES AND SECURITY INCIDENTS

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

A. ***Initial Notice to DHCS:***
The County Department/Agency shall notify DHCS using DHCS' online incident reporting portal of any suspected security incident, intrusion, or unauthorized access, use, or disclosure of Medi-Cal PII or potential loss of Medi-Cal PII. When making notification, the following applies:

1. If a suspected security incident involves Medi-Cal PII provided or verified by SSA, the County Department/Agency shall immediately notify DHCS upon discovery. For more information on SSA data, please see the Definition section of this Agreement.

2. If a suspected security incident does not involve Medi-Cal PII provided or verified by SSA, the County Department/Agency shall notify DHCS promptly and in no event later than one working day of discovery of:

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

Notice to DHCS shall include all information known at the time the incident is reported. The County Department/Agency can submit notice via the DHCS incident reporting portal which is available online at: https://www.dhcs.ca.gov/formsandpubs/laws/priv/Pages/default.aspx

If DHCS' online incident reporting portal is unavailable, notice to DHCS can instead be made via email using the DHCS Privacy Incident Report (PIR) form. The email address to submit a PIR can be found on the PIR and in subsection H of this section. The County Department/Agency shall use the most current version of the PIR, which is available online at: https://www.dhcs.ca.gov/formsandpubs/laws/priv/Documents/Privacy-Incident-Report-PIR.pdf.

If the County Department/Agency is unable to notify DHCS the via the Incident Reporting Portal or email, notification can be made by telephone using the contact information listed in subsection H.

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

Upon discovery of a breach, security incident, intrusion, or unauthorized access, use, or disclosure of Medi-Cal PII, the County Department/Agency shall take:

1. Prompt corrective action to mitigate any risks or damages involved with the security incident or breach; and

2. Any action pertaining to such unauthorized disclosure required by applicable Federal and State laws and regulations.

B. ***Investigation of Security Incident or Breach.*** The County Department/Agency shall immediately investigate such a security incident, breach, or unauthorized use of Medi-Cal PII.

C. ***Complete Report.*** Within ten (10) working days of the discovery the County Department/Agency shall provide any additional information related to the incident requested by DHCS. The County Department/Agency shall make reasonable efforts to provide DHCS with such information.

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

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

D. ***Notification of Individuals.*** If the cause of a breach is solely attributable to County Department/Agency or its agents, County Department/Agency shall notify individuals accordingly and shall pay all costs of such notifications as well as any costs associated with the breach. The notifications shall comply with applicable federal and state law. DHCS shall approve the time, manner, and content of any such notifications and their review and approval must be obtained before the notifications are made. DHCS and the County Department/Agency shall work together to ensure that notification of individuals is done in compliance with statutory deadlines within applicable federal and state law.

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

1. All notifications (regardless of breach status) regarding beneficiaries' Medi-Cal PII shall comply with the requirements set forth in Section

1798.29 of the California Civil Code and Section 17932 of Title 42 of United States Code, inclusive of its implementing regulations, including but not limited to the requirement that the notifications be made without unreasonable delay and in no event later than **sixty (60) calendar days** from discovery.

E. ***Responsibility for Reporting of Breaches***

1. ***Breach Attributable to County Department/Agency.*** If the cause of a breach of Medi-Cal PII is attributable to the County Department/Agency or its agents, subcontractors, or vendors, the County Department/Agency shall be responsible for all required reporting of the breach.

2. ***Breach Attributable to DHCS.*** If the cause of the breach is attributable to DHCS, DHCS shall be responsible for all required reporting of the breach.

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

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

1. Electronically submit a single sample copy of the security breach notification, excluding any personally identifiable information, to the Attorney General pursuant to the format, content, and timeliness provisions of Section 1798.29, subdivision (e). County Department/Agency shall inform the DHCS Privacy Officer of the time, manner, and content of any such submissions prior to the transmission of such submissions to the Attorney General; or

2. Cooperate with and assist DHCS in its submission of a sample copy of the notification to the Attorney General.

H. ***DHCS Contact Information.*** The County Department/Agency shall utilize the below contact information to direct all communication/notifications of breach and security incidents to DHCS. DHCS reserves the right to make changes to the contact information by giving written notice to the County

Department/Agency. Said changes shall not require an amendment to this Agreement or any other agreement into which it is incorporated.

DHCS Breach and Security Incident Reporting
Privacy Officer c/o Data Privacy Unit Department of Health Care Services P.O. Box 997413, MS 0011 Sacramento, CA 95899-7413 Email: incidents@dhcs.ca.gov Telephone: (916) 445-4646 *The preferred method of communication is email, when available. Do not include any Medi-Cal PII unless requested by DHCS.*

IX. DHCS PSA CONTACTS

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

PSA Inquires and Questions
Department of Health Care Services Medi-Cal Eligibility Division 1501 Capitol Avenue, MS 4607 P.O. Box 997417 Sacramento, CA 95899-7417 Email: countypsa@dhcs.ca.gov

X. COMPLIANCE WITH SSA AGREEMENT

The County Department/Agency agrees to comply with applicable privacy and security requirements in the Computer Matching and Privacy Protection Act Agreement (CMPPA) between SSA and the California Health and Human Services Agency (CalHHS), in the Information Exchange Agreement (IEA) between SSA and DHCS, and in the Electronic Information Exchange Security Requirements and Procedures for State and Local Agencies Exchanging Electronic Information with SSA (TSSR), which

are incorporated into this Agreement within section V. Technical Security Controls and Exhibit A (available upon request).
If there is any conflict between a privacy and security standard in the CMPPA, IEA or TSSR, and a standard in this Agreement, the most stringent standard shall apply. The most stringent standard means the standard which provides the greatest protection to Medi-Cal PII.

If SSA changes the terms of its agreement(s) with DHCS, DHCS will, as soon as reasonably possible after receipt, supply copies to County Welfare Directors Association (CWDA) and the County Department/Agency or its designee as well as DHCS' proposed target date for compliance. For a period of thirty (30) days, DHCS will accept input from CWDA and the County Department/Agency or its designee on the proposed target date and make adjustments, if appropriate. After the thirty (30) day period, DHCS will submit the proposed target date to SSA, which will be subject to adjustment by SSA. Once a target date for compliance is determined by SSA, DHCS will supply copies of the changed agreement to CWDA and the County Department/Agency or its designee, along with the compliance date expected by SSA. If the County Department/Agency is not able to meet the SSA compliance date,, the County Department/Agency will be asked to develop a POA&M detailing a concrete roadmap to becoming fully compliant with the policy's standard. The POA&M must be provided to DHCS for review and approval. Any County Department/Agency who is under a POA&M will be required to provide quarterly updates to DHCS until the fully compliant.

A copy of Exhibit A can be requested by authorized County Department/Agency individuals from DHCS using the contact information listed in Section XI of this Agreement.

XI. COMPLIANCE WITH DEPARTMENT OF HOMELAND SECURITY AGREEMENT

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

If DHS-USCIS changes the terms of its agreement(s) with DHCS, DHCS will, as soon as reasonably possible after receipt, supply copies to the CWDA and the County Department/Agency or its designee as well as DHCS' proposed target date for compliance. For a period of thirty (30) days, DHCS will accept input from CWDA and the County Department/Agency or its designee on the proposed target date and make adjustments, if appropriate. After the 30-day period, DHCS will submit the proposed target date to DHS-USCIS, which will be subject to adjustment by DHS-USCIS. Once

a target date for compliance is determined by DHS-USCIS, DHCS will supply copies of the changed agreement to CWDA and the County Department/Agency or its designee, along with the compliance date expected by DHS-USCIS. If the County Department/Agency is not able to meet the DHS-USCIS compliance date, the POA&M must be provided to DHCS for review and approval. Any County Department/Agency who is under a POA&M will be required to provide quarterly updates to DHCS until the fully compliant.

A copy of Exhibit B can be requested by authorized County Department/Agency individuals from DHCS using the contact information listed in Section IX of this Agreement.

XII. COUNTY DEPARTMENT'S/AGENCY'S AGENTS, SUBCONTRACTORS, AND VENDORS

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

County Departments/Agencies who would like assistance or guidance with this requirement are encouraged to contact DHCS via the PSA inbox at CountyPSA@dhcs.ca.gov.

XIII. ASSESSMENTS AND REVIEWS

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

XIV. ASSISTANCE IN LITIGATION OR ADMINISTRATIVE PROCEEDINGS

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

XV. AMENDMENT OF AGREEMENT

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

XVI. TERMINATION

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

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

XVII. TERMINATION FOR CAUSE

Upon DHCS' knowledge of a material breach or violation of this Agreement by the County Department/Agency, DHCS may provide an opportunity for the County Department/Agency to cure the breach or end the violation and may terminate this Agreement if the County Department/Agency does not cure the breach or end the

violation within the time specified by DHCS. This Agreement may be terminated immediately by DHCS if the County Department/Agency has breached a material term and DHCS determines, in its sole discretion, that cure is not possible or available under the circumstances. Upon termination of this Agreement, the County Department/Agency shall return or destroy all Medi-Cal PII in accordance with Section VII, above. The provisions of this Agreement governing the privacy and security of the Medi-Cal PII shall remain in effect until all Medi-Cal PII is returned or destroyed and DHCS receives a certificate of destruction.

MEDI-CAL PRIVACY & SECURITY AGREEMENT NO.: 24 - 19

XVIII. SIGNATORIES

The signatories below warrant and represent that they have the competent authority on behalf of their respective agencies to enter into the obligations set forth in this Agreement.

The authorized officials whose signatures appear below have committed their respective agencies to the terms of this Agreement. The contract is effective on September 1, 2024.

For the County of Los Angeles,

Department/Agency of Public Social Services,

Jackie Contreras Digitally signed by Jackie Contreras Date: 2024.10.09 12:26:29 -07'00' _____
(Signature) (Date)

Jackie Contreras, Ph.D. Director
(Name) (Title)

For the Department of Health Care Services,

DocuSigned by: Sarah Crow A813B5EEF5B5445... October 10, 2024
(Signature) (Date)

Sarah Crow Medi-Cal Eligibility Division Chief
(Name) (Title)

EXHIBIT A

Exhibit A consists of the current versions of the following documents, copies of which can be requested by the County Department/Agency information security and privacy staff, or other authorized county official from DHCS by using the contact information listed in Section IX of this Agreement.

- Computer Matching and Privacy Protection Act Agreement between the SSA and California Health and Human Services Agency
- Information Exchange Agreement between SSA and DHCS
- Electronic Information Exchange Security Requirements and Procedures for State and Local Agencies Exchanging Electronic Information with the SSA (TSSR)

EXHIBIT B

Exhibit B consists of the current version of the following document, a copy of which can be requested by the County Department/Agency information security and privacy staff, or other authorized county official from DHCS by using the contact information listed in Section IX of this Agreement.

- Computer Matching Agreement between the Department of Homeland Security, United States Citizenship and Immigration Services (DHS-USCIS) and California Department of Health Care Services (DHCS)

EXHIBIT C

Exhibit C consists of the current version of the SIMM-5300-A, a copy of which can be requested by the County Department/Agency information security and privacy staff, or other authorized county official from DHCS by using the contact information listed in Section IX of this Agreement. The SIMM-5300-A can be used as guidance for implementing security controls found in NIST SP 800-53.

ELECTRONIC INFORMATION EXCHANGE SECURITY REQUIREMENTS AND PROCEDURES FOR STATE AND LOCAL AGENCIES EXCHANGING ELECTRONIC INFORMATION WITH THE SSA (TSSR)

CONFIDENTIAL DOCUMENT – TO BE SENT VIA ENCRYPTED E-MAIL

REST OF PAGE INTENTIONALLY LEFT BLANK

CONTRACTOR'S EEO CERTIFICATION

Contractor Name

Address

Internal Revenue Service Employer Identification Number

GENERAL CERTIFICATION

In accordance with Section 4.32.010 of the Code of the County of Los Angeles, the contractor, supplier, or vendor certifies and agrees that all persons employed by such firm, its affiliates, subsidiaries, or holding companies are and will be treated equally by the firm without regard to or because of race, religion, ancestry, national origin, or sex and in compliance with all anti-discrimination laws of the United States of America and the State of California.

CONTRACTOR'S SPECIFIC CERTIFICATIONS

1.	The Contractor has a written policy statement prohibiting discrimination in all phases of employment.	Yes ☐	No ☐
2.	The Contractor periodically conducts a self analysis or utilization analysis of its work force.	Yes ☐	No ☐
3.	The Contractor has a system for determining if its employment practices are discriminatory against protected groups.	Yes ☐	No ☐
4.	Where problem areas are identified in employment practices, the Contractor has a system for taking reasonable corrective action, to include establishment of goals or timetables.	Yes ☐	No ☐

Authorized Official's Printed Name and Title

Authorized Official's Signature

Date

CONTRACTOR'S NON-DISCRIMINATION IN SERVICES CERTIFICATION

Contractor's Name _____

Address _____

Internal Revenue Service Employer Identification Number_____

GENERAL

In accordance with Subchapter VI and VII of the *Civil Rights Act of 1964*, *Section 504* of the *Rehabilitation Act of 1973*, as amended, the *Age Discrimination Act of 1975*, the *Food Stamp Act of 1977*, and the *Americans with Disabilities Act of 1990,* the Contractor, supplier, or vendor certifies and agrees that all persons serviced by such firm, its affiliates, subsidiaries, or holding companies are and will be treated equally by the firm without regard to or because of race, color, religion, ancestry, national origin, age, condition of disability, marital status, political affiliation, or sex and in compliance with all anti-discrimination laws of the United States of America and the State of California.

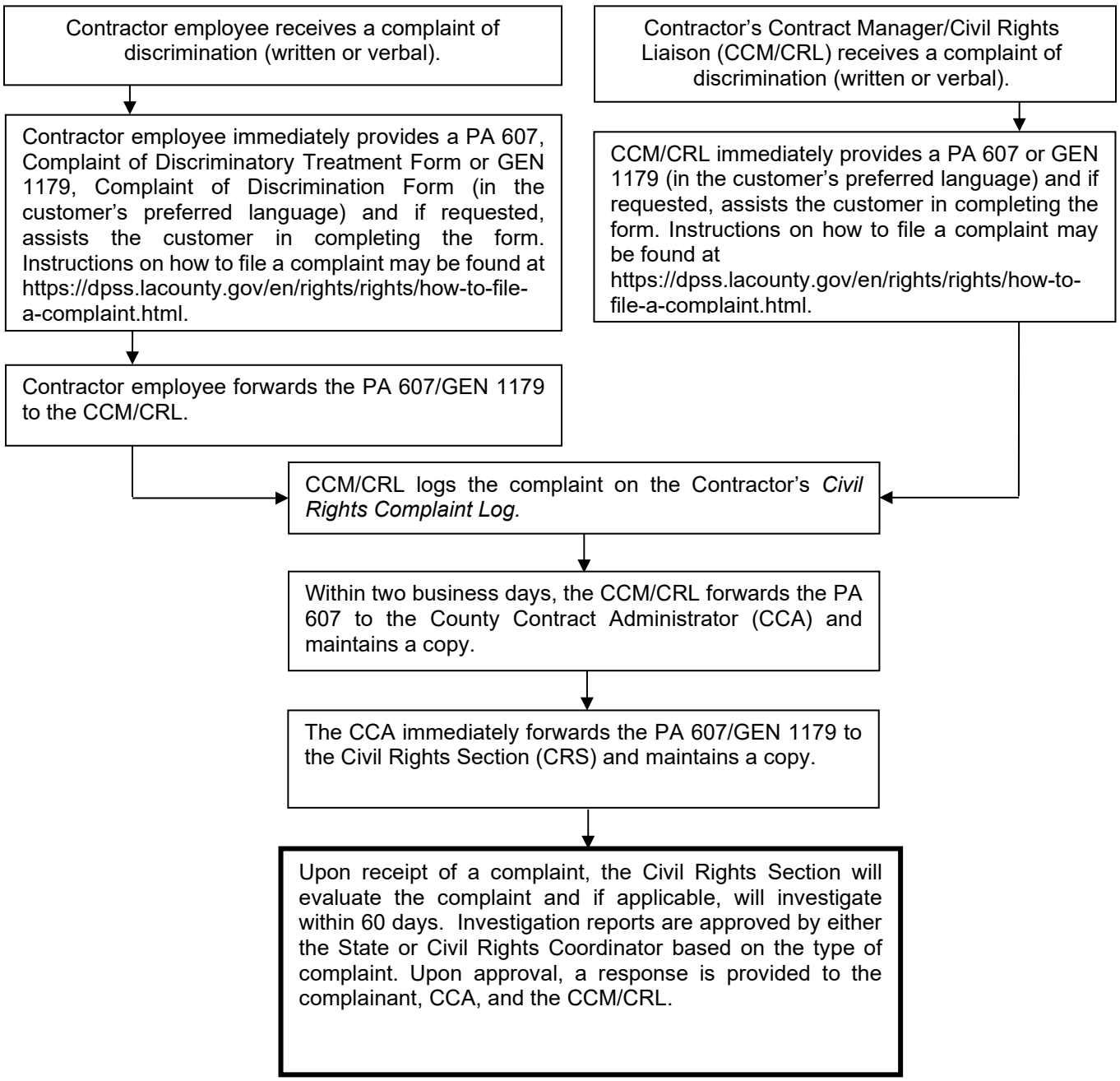
CERTIFICATION

	(Circle one)	
1. The Contractor has a written policy statement prohibiting discrimination in providing services and benefits.	Yes	No
2. The Contractor periodically monitors the equal provision of services to ensure nondiscrimination.	Yes	No
3. Where problem areas are identified in equal provisions of services and benefits, the Contractor has a system for taking reasonable corrective action within a specified length of time.	Yes	No

_____
Printed Name and Title of Authorized Signer

_____ _____
Signature Date

CIVIL RIGHTS COMPLAINT FLOWCHART PROCESS FOR CONTRACTORS



Rev. 06/2024

Title 2 ADMINISTRATION
Chapter 2.203.010 through 2.203.090
CONTRACTOR EMPLOYEE JURY SERVICE

2.203.010 Findings.

The board of supervisors makes the following findings. The county of Los Angeles allows its permanent, full-time employees unlimited jury service at their regular pay. Unfortunately, many businesses do not offer or are reducing or even eliminating compensation to employees who serve on juries. This creates a potential financial hardship for employees who do not receive their pay when called to jury service, and those employees often seek to be excused from having to serve. Although changes in the court rules make it more difficult to excuse a potential juror on grounds of financial hardship, potential jurors continue to be excused on this basis, especially from longer trials. This reduces the number of potential jurors and increases the burden on those employers, such as the county of Los Angeles, who pay their permanent, full-time employees while on juror duty. For these reasons, the county of Los Angeles has determined that it is appropriate to require that the businesses with which the county contracts possess reasonable jury service policies. (Ord. 2002-0015 § 1 (part), 2002)

2.203.020 Definitions.

The following definitions shall be applicable to this chapter:

A. "Contractor" means a person, partnership, corporation or other entity which has a contract with the county or a subcontract with a county contractor and has received or will receive an aggregate sum of $50,000 or more in any 12-month period under one or more such contracts or subcontracts.

B. "Employee" means any California resident who is a full-time employee of a contractor under the laws of California.

C. "Contract" means any agreement to provide goods to, or perform services for or on behalf of, the county but does not include:

1. A contract where the board finds that special circumstances exist that justify a waiver of the requirements of this chapter; or
2. A contract where federal or state law or a condition of a federal or state program mandates the use of a particular contractor; or
3. A purchase made through a state or federal contract; or
4. A monopoly purchase that is exclusive and proprietary to a specific manufacturer, distributor, or reseller, and must match and inter-member with existing supplies, equipment or systems maintained by the county pursuant to the Los Angeles County Purchasing Policy and Procedures Manual, Section P-3700 or a successor provision; or
5. A revolving fund (petty cash) purchase pursuant to the Los Angeles County Fiscal Manual, Section 4.4.0 or a successor provision; or
6. A purchase card purchase pursuant to the Los Angeles County Purchasing Policy and Procedures Manual, Section P-2810 or a successor provision; or
7. A non-agreement purchase with a value of less than $5,000 pursuant to the Los Angeles County Purchasing Policy and Procedures Manual, Section A-0300 or a successor provision; or

8. A bona fide emergency purchase pursuant to the Los Angeles County Purchasing Policy and Procedures Manual, Section PP-1100 or a successor provision.

D. "Full time" means 40 hours or more worked per week, or a lesser number of hours if:

1. The lesser number is a recognized industry standard as determined by the chief administrative officer, or

2. The contractor has a long-standing practice that defines the lesser number of hours as full time.

E. "County" means the county of Los Angeles or any public entities for which the board of supervisors is the governing body. (Ord. 2002-0040 § 1, 2002: Ord. 2002-0015 § 1 (part), 2002)

2.203.030 Applicability.

This chapter shall apply to contractors who enter into contracts that commence after July 11, 2002. This chapter shall also apply to contractors with existing contracts which are extended into option years that commence after July 11, 2002. Contracts that commence after May 28, 2002, but before July 11, 2002, shall be subject to the provisions of this chapter only if the solicitations for such contracts stated that the chapter would be applicable. (Ord. 2002-0040 § 2, 2002: Ord. 2002-0015 § 1 (part), 2002)

2.203.040 Contractor Jury Service Policy.

A contractor shall have and adhere to a written policy that provides that its employees shall receive from the contractor, on an annual basis, no less than five days of regular pay for actual jury service. The policy may provide that employees deposit any fees received for such jury service with the contractor or that the contractor deduct from the employees' regular pay the fees received for jury service. (Ord. 2002-0015 § 1 (part), 2002)

2.203.050 Other Provisions.

A. Administration. The chief administrative officer shall be responsible for the administration of this chapter. The chief administrative officer may, with the advice of county counsel, issue interpretations of the provisions of this chapter and shall issue written instructions on the implementation and ongoing administration of this chapter. Such instructions may provide for the delegation of functions to other county departments.

B. Compliance Certification. At the time of seeking a contract, a contractor shall certify to the county that it has and adheres to a policy consistent with this chapter or will have and adhere to such a policy prior to award of the contract. (Ord. 2002-0015 § 1 (part), 2002)

2.203.060 Enforcement and Remedies.

For a contractor's violation of any provision of this chapter, the county department head responsible for administering the contract may do one or more of the following:

1. Recommend to the board of supervisors the termination of the contract; and/or,

2. Pursuant to chapter 2.202, seek the debarment of the contractor. (Ord. 2002-0015 § 1 (part), 2002)

2.203.070. Exceptions.

A. Other Laws. This chapter shall not be interpreted or applied to any contractor or to any employee in a manner inconsistent with the laws of the United States or California.

B. Collective Bargaining Agreements. This chapter shall be superseded by a collective bargaining agreement that expressly so provides.

C. Small Business. This chapter shall not be applied to any contractor that meets all of the following:

1. Has ten or fewer employees during the contract period; and,

2. Has annual gross revenues in the preceding twelve months which, if added to the annual amount of the contract awarded, are less than $500,000; and,

3. Is not an affiliate or subsidiary of a business dominant in its field of operation.

"Dominant in its field of operation" means having more than ten employees and annual gross revenues in the preceding twelve months which, if added to the annual amount of the contract awarded, exceed $500,000.

"Affiliate or subsidiary of a business dominant in its field of operation" means a business which is at least 20 percent owned by a business dominant in its field of operation, or by partners, officers, directors, majority stockholders, or their equivalent, of a business dominant in that field of operation. (Ord. 2002-0015 § 1 (part), 2002)

2.203.090. Severability.

If any provision of this chapter is found invalid by a court of competent jurisdiction, the remaining provisions shall remain in full force and effect. (Ord. 2002-0015 § 1 (part), 2002)

CERTIFICATION OF NO CONFLICT OF INTEREST

The Los Angeles County Code, Section 2.180.010, provides as follows:

CONTRACTS PROHIBITED

Notwithstanding any other section of this Code, the County shall not contract with, and shall reject any SOQs submitted by, the persons or entities specified below, unless the Board of Supervisors finds that special circumstances exist which justify the approval of such contract:

1. Employees of the County or of public agencies for which the Board of Supervisors is the governing body;

2. Profit-making firms or businesses in which employees described in number 1 serve as officers, principals, partners, or major shareholders;

3. Persons who, within the immediately preceding 12 months, came within the provisions of number 1, and who:

    a. Were employed in positions of substantial responsibility in the area of service to be performed by the contract; or

    b. Participated in any way in developing the contract or its service specifications; and

4. Profit-making firms or businesses in which the former employees, described in number 3, serve as officers, principals, partners, or major shareholders.

Contracts submitted to the Board of Supervisors for approval or ratification shall be accompanied by an assurance by the submitting department, district or agency that the provisions of this section have not been violated.

_____
Contractor Name

_____
Contractor Official Title

_____
Official's Signature

ZERO TOLERANCE POLICY ON HUMAN TRAFFICKING CERTIFICATION

Company Name:		
Company Address:		
City:	State:	Zip Code:
Telephone Number:	Email address:	
Solicitation/Contract for _____ Services		

CONTRACTOR CERTIFICATION

Los Angeles County has taken significant steps to protect victims of human trafficking by establishing a zero tolerance policy on human trafficking that prohibits contractors found to have engaged in human trafficking from receiving contract awards or performing services under a County contract.

Contractor acknowledges and certifies compliance with Section 8.53 (Compliance with County's Zero Tolerance Policy on Human Trafficking) of the proposed Contract and agrees that vendor or a member of his staff performing work under the proposed Contract will be in compliance. Contractor further acknowledges that noncompliance with the County's Zero Tolerance Policy on Human Trafficking may result in rejection of any proposal, or cancellation of any resultant Contract, at the sole judgment of the County.

I declare under penalty of perjury under the laws of the State of California that the information herein is true and correct and that I am authorized to represent this company.

Print Name:	Title:
Signature:	Date:

CERTIFICATION REGARDING DEBARMENT, SUSPENSION, INELIGIBILITY AND VOLUNTARY EXCLUSION - LOWER TIERED COVERED TRANSACTIONS (45 C.F.R. PART 76)

Instructions for Certification Regarding Debarment, Suspension, Ineligibility and Voluntary Exclusion -- Lower Tiered Covered Transactions (45 C.F.R. Part 76)

1. This certification is a material representation of fact upon which reliance was placed when this transaction was entered into. If it is later determined that Proposer knowingly rendered an erroneous certification, in addition to other remedies available to the Federal Government, the department or agency with which this transaction originated may pursue available remedies, including suspension and/or debarment.

2. Proposer shall provide immediate written notice to the person to whom this proposal is submitted if at any time Proposer learns that its certification was erroneous when submitted or has become erroneous by reason of changed circumstances.

3. The terms “covered transaction,” “debarred,” “suspended,” “ineligible,” “lower tier covered transaction,” “Participant,” “person,” “primary covered transaction, “principal,” “proposal,” and “voluntarily excluded,” as used in this certification, have the meaning set out in the Definitions and Coverage sections of rules implementing Executive Order 12549. You may contact the person to which this proposal is submitted for assistance in obtaining a copy of those regulations.

4. Proposer agrees by submitting this proposal that, should the proposed covered transaction be entered into, it shall not knowingly enter into any lower tier covered transaction with a person who is proposed for debarment under 48 CFR part 9, subpart 9.4, debarred, suspended, declared ineligible, or voluntarily excluded from participation in this covered transaction, unless authorized by the department or agency with which this transaction originated.

5. Proposer further agrees by submitting this proposal that it will include the provision entitled Certification Regarding Debarment, Suspension, Ineligibility and Voluntary Exclusion --Lower Tier Covered Transaction (45 C.F.R. Part 76),” as set forth in the text of the Sample Master Agreement attached to the Request for Statement of Qualifications, without modification, in all lower tier covered transactions and in all solicitations for lower tier covered transactions.

6. Proposer acknowledges that a participant in a covered transaction may rely upon a certification of a prospective Participant in a lower tier covered transaction that it is not proposed for debarment under 48 C.F.R. part 9, subpart 9.4, debarred, suspended, ineligible, or voluntarily excluded from covered transaction, unless it knows that the certification is erroneous.

   Proposer acknowledges that a Participant may decide the methods and frequency by which it determines the eligibility of its principals. Proposer acknowledges that

each Participant may, but is not required to; check the List of Parties Excluded from Federal Procurement and Non-procurement Programs.

7. Nothing contained in the foregoing shall be construed to require establishment of a system of records in order to render in good faith the required certification. The knowledge and information of a participant is not required to exceed that which is normally possessed by a prudent person in the ordinary course of business dealings.

8. Expert for transactions authorized under paragraph 4 of these instructions, if a participant in a covered transaction knowingly enters into a lower tier covered transaction with a person who is proposed for debarment under 48 CFR part 9, subpart 9.4, suspended, debarred, ineligible, or voluntarily excluded from participation in this transaction, in addition to other remedies available to the Federal Government, the department or agency with which this transaction originated may pursue available remedies, including suspension and/or debarment.

9. Where Proposer and/or its subcontractor/Subcontractor(s) is or are unable to certify to any of the statements in this Certification, Proposer shall attach a written explanation to its proposal in lieu of submitting this Certification. Proposer's written explanation shall describe the specific circumstances concerning the inability to certify. It further shall identify any owner, officer, partner, director, or other principal of the Proposer and/or subcontractor/Subcontractor who is currently suspended, debarred, ineligible, or excluded from securing federally funded contracts. The written explanation shall provide that person's or those persons' job description(s) and function(s) as they relate to the agreement which is being solicited by this Request for Statement of Qualifications.

Certification Regarding Debarment, Suspension, Ineligibility and Voluntary Exclusion--Lower Tier Covered transactions (45 C.F.R. Part 76)

Proposer hereby certifies that neither it nor any of its owners, officers, partners, directors, other principals or subcontractor/Subcontractors is currently debarred, suspended, proposed for debarment, declared ineligible or excluded from securing federally funded contracts by any federal department or agency.

_____ _____

Dated Signature of Authorized Representative

_____

Title of Authorized Representative

_____

Printed Name of Authorized Representative

FUNDING FOR COMMUNITY SERVICES BLOCK GRANT PROGRAM BY SUPERVISORIAL DISTRICT

Supervisorial District	Percent of CAA Population
1	32.4%
2	24.3%
3	3.7%
4	16.8%
5	22.8%
Total	**100%**