AMENDMENT ONE TO CONTRACT

BETWEEN

COUNTY OF ORANGE

AND

ARBOR E&T, LLC DBA EQUUS WORKFORCE SOLUTIONS

FOR THE PROVISION OF INTEGRATED JOB SERVICES

THIS AMENDMENT ONE, made and entered into upon execution of all necessary signatures, is to that certain CONTRACT Number WDM0922 between the parties hereto, hereinafter referred to as the "Contract" and is by and between the COUNTY OF ORANGE, hereinafter referred to as "COUNTY," and ARBOR E&T, LLC DBA EQUUS WORKFORCE SOLUTIONS, hereinafter referred to as "CONTRACTOR." COUNTY and CONTRACTOR may be referred to individually as "Party" and collectively as "the Parties."

W I T N E S S E T H

WHEREAS, on July 1, 2022, COUNTY and CONTRACTOR entered into an Contract for the provision of Integrated Job Services, for the term of July 1, 2022, through June 30, 2025;

WHEREAS, COUNTY desires to amend Subparagraphs 19.4, 21.3.1 and Paragraph 32 of the Contract; and amend Subparagraph 4.2 of Attachment A of the Contract;

WHEREAS, COUNTY desires to replace Attachment B in its entirety, replace Attachment D of the Contract in its entirety, and add Attachment E to the Contract;

WHEREAS, CONTRACTOR agrees to such amendments and to continue to provide such services under the terms and conditions set forth in this Contract; and

ACCORDINGLY, THE PARTIES AGREED AS FOLLOWS:

1. Subparagraph 19.4 of the Contract is hereby amended to read as follows:

   19.4   Use of COUNTY Computer Equipment

   COUNTY intends to permit CONTRACTOR the use of computer equipment provided by ADMINISTRATOR.   Said computer equipment shall be used solely by employees of CONTRACTOR while performing their assigned duties pursuant to this Contract, and shall remain the property of COUNTY. CONTRACTOR shall ensure that each of its employees, volunteers, consultants, or agents that have access to COUNTY facilities and/or data contained in ADMINISTRATOR's Computer Information System completes information security and computer usage training provided by ADMINISTRATOR, and adheres to the provisions in Attachments B, C, D and E, to this Contract, signs and adheres to the provisions in SSA Information Technology Security and Usage Agreement as referenced and included in Attachment B, and adheres to any subsequent contracts required by federal or State laws or regulations. CONTRACTOR's failure to have all CONTRACTOR employees that have access to COUNTY's facilities and/or data execute the contracts and/or complete the training shall constitute a breach of this Contract.

2. Subparagraph 21.3.1 of the Contract is hereby amended to read as follows:

   21.3.1   CONTRACTOR   shall   submit   monthly   claims   to   be   received   by ADMINISTRATOR no later than the twentieth (20th) calendar day of the month for expenses incurred in the preceding month, except as detailed below in Subparagraph 21.3.4. In the event the twentieth (20th) calendar day falls on a weekend or COUNTY holiday, CONTRACTOR shall submit the claim the next business day. COUNTY holidays include New Year's Day, Martin Luther King Jr. Day, President Lincoln's Birthday, Presidents' Day, Memorial Day, Independence Day, Labor Day, Native American Day, Veterans Day, Thanksgiving Day, Friday after Thanksgiving Day, and Christmas Day.

3. Paragraph 32 of the Contract is hereby amended to read as follows:

   32.   SECURITY

   Contractor shall abide by the requirements in Attachments D and E.

4. Subparagraph 4.2 of Attachment A of the Contract is hereby amended to read as follows:

4.2 CONTRACTOR's holiday schedule shall not exceed COUNTY's holiday schedule which is as follows: New Year's Day, Martin Luther King Jr. Day, President Lincoln's Birthday, Presidents' Day, Memorial Day, Independence Day, Labor Day, Native American Day, Veterans Day, Thanksgiving Day, Friday after Thanksgiving Day, and Christmas Day. CONTRACTOR shall obtain prior written approval from ADMINISTRATOR for any closure outside of COUNTY's holiday schedule and the hours listed in Subparagraph 4.1 of this Attachment A. Any unauthorized closure shall be deemed a material breach of this Contract, pursuant to Paragraph 20, and shall not be reimbursed.

5. Attachment B of the Contract is hereby replaced in its entirety and is attached as follows.

6. Attachment D of the Contract is hereby replaced in its entirety and is attached as follows.

7. Attachment E is hereby added to the Contract and is attached as follows.

8. The Parties agree that separate copies of this Amendment may be signed by each of the Parties, and this Amendment will have the same force and effect as if the original had been signed by all Parties.

9. All other terms and conditions of the Contract shall remain the same and in full force and in effect.

IN WITNESS WHEREOF, the Parties hereto have executed this Amendment One to Contract on the date set forth opposite their signatures. If Contractor is a corporation, Contractor shall provide two signatures as follows: 1) the first signature must be either the Chairman of the Board, the President, or any Vice President; 2) the second signature must be that of the Secretary, an Assistant Secretary, the Chief Financial Officer, or any Assistant Treasurer. In the alternative, a single corporate signature is acceptable when accompanied by a corporate resolution or by-laws demonstrating the legal authority of the signature to bind the company.

Contractor: ARBOR E&T, LLC DBA EQUUS WORKFORCE SOLUTIONS

Mark Douglass

Nicole Ganier

Print Name

Mark Douglass
CA5DDAD2E622464...

Nicole Ganier
461E66B74DDE462...

Signature

President

Vice President

Title

11/9/2023 | 9:54:18 AM PST

11/9/2023 | 9:01:37 AM PST

Date

County of Orange, a political subdivision of the State of California

Deputized Designee Signature:

Desiree Mor

Print Name

Desiree Mor
833175226ABA4B5...

Signature

Deputy Purchasing Agent

Title

11/9/2023 | 11:51:24 AM PST

Date

APPROVED AS TO FORM
COUNTY COUNSEL
COUNTY OF ORANGE, CALIFORNIA

Carolyn S. Frost

Print Name

Carolyn S. Frost
D3AB98D76D0B425...

Signature

Deputy County Counsel

Title

10/17/2023 | 10:04:07 AM PDT

Date

Attachment B

SOCIAL SERVICES AGENCY POLICY AND PROCEDURE I 6:

INFORMATION TECHNOLOGY SECURITY AND USAGE

I. PURPOSE

To protect the integrity of the Social Services Agency's (SSA) Information Technology (IT) infrastructure, ensure its availability, reliability, accessibility, and prevent unauthorized disclosure of Confidential Information, including Personally Identifiable Information (PII). Additionally, this policy defines required responsibilities for all users of the SSA information technology infrastructure and supplements the County of Orange Information Technology Policies.

II. DEFINITIONS

Confidential Information is defined as information that must be protected from unauthorized disclosure or public release. Examples include, but are not limited to the following:

1. Client case records
2. Employment Records
3. Payroll and other financial information
4. Other sensitive or business-related information that is not intended for wide distribution

Personally Identifiable Information (PII) is information that can be used, alone or in conjunction with any other information, to identify a specific individual. PII includes any information that can be used to search for or identify individuals or can be used to access their files. Examples of PII may include, but are not limited to name, Social Security Number, Social Security benefit data, date of birth, official state or government issued driver's license, or identification number. PII is a subset of Confidential Information.

SSA Workforce Members include full-time, part-time, and extra-help County of Orange SSA employees, contracted staff, interns, volunteers, and all other authorized individuals with access to SSA's information technology infrastructure.

III. POLICY

SSA workforce members shall adhere to applicable SSA and County policies, including, but not limited to, the following: County of Orange Information Technology Usage Policy, state and federal statutes including (California Welfare and Institutions Code, Division 9, Part 2, Chapter 5), and regulations relating to information technology security, privacy, and confidentiality of information as each may now exist or be amended in the future.

Unless within the scope of job responsibility, any use of Confidential Information will be considered a violation of this policy and will be subject to immediate revocation of the user's access to SSA network and associated applications. SSA workforce members may be subject to disciplinary action including suspension, termination, civil, and/or criminal prosecution for violating governing security and usage policies, statutes, and regulations (e.g., and the County of Orange Information Technology Usage Policy (Attachment I).

All SSA workforce members shall:

1. Keep user Identification(s) (ID)/Username(s) and passwords confidential and secured at all times.

2. Never share username(s)/password(s).

3. Immediately change passwords and notify IT and the supervisor if an account has been compromised.

4. Limit usage of County data, systems, and equipment to currently assigned job duties and responsibilities.

5. County-issued IT equipment shall not be used outside the State of California without express supervisory permission.

6. Use County resources, such as data and information, for County business objectives only. Use of these resources for private or personal gain is prohibited and may be subject to administrative, civil, and criminal penalties (e.g., California Penal Code, Section 502).

7. Protect Confidential Information of clients/customers to prevent unauthorized disclosure. Only the minimum amount of Confidential Information necessary for business operations should be copied, downloaded, exported, or stored on any electronic device or in paper format. Any compromise of Confidential Information and/or PII shall be immediately reported to the supervisor.

8. Request software installations/downloads on SSA computers, laptops, tablets and other devices from an authorized agent of the OC Information Technology (OCIT) team. DO NOT INSTALL ANY software/application into County-issued devices. Requests can be submitted through the Service Now portal at https://ismcg.service-now.com/oc?id=oc_index or by calling the Central IT Service Desk at (844) 834-2449.

   Note: pre-approved applications for County-issued cell phones can be downloaded from the Company Portal (Comp Portal) application without seeking approval from OCIT.

9. Seek permission from OCIT prior to copying a County-owned software/application.

10. Use County electronic communication systems for business use only; any personal use during nonworking hours shall be in strict compliance with policy and shall not disrupt or interfere with County operations or job responsibilities. If there is any doubt about whether an activity is appropriate, consult with your supervisor or manager.

11. Adhere to related SSA policies, including P&P F21 Privacy and Security Incidents of Personally Identifying Information (PII) and Confidential Information and P&P D20 Remote Work.

IV. PROCEDURE

SSA Employees

The following steps shall be undertaken to ensure that the above policy is enforced to all SSA County employees. Prior to a new employee gaining access to Confidential Information, the SSA Human Resources (HR) representative or designee shall:

1. Provide new employees with access to the SSA I-6 Policy and Procedures document, the County of Orange Information Technology Usage Policy (Attachment I) with instructions for the new employee to read and sign the SSA Information Technology Security and Usage Agreement (Attachment II). Upon the new employee's signing of SSA Information Technology Usage Agreement form, the HR representative or designee shall sign the completed form to acknowledge receipt.

2. Have the new employee read and sign the Orange County Social Services Agency Confidentiality of Client Information (Attachment III).

3. Confirm the new employee has completely reviewed the SSA Information Security Rules of the Road (Attachment IV) located in the Training section of the SSA Intranet at http://ocssa/intranet/ssa/Training.

4. File the signed SSA Information Technology Usage Agreement (Attachment II), the signed Orange County Social Services Agency Confidentiality of Client Information (Attachment III) and documentation of completion of SSA Information Security Rules of the Road (Attachment IV) in the employee's personnel file.

SSA Contracted Employee, Volunteer, Intern, and All Other Non-County Employees

The supervisor of an SSA contracted employee, volunteer, intern, and all other non-County employees shall undertake the following steps to ensure the above policy is enforced. Prior to a workforce member gaining access to Confidential Information, provide them with the following documents to read:

1. Administrative Policies and Procedures Manual I-6 Information Technology Security and Usage. The new workforce member shall document that they have read, understand and will adhere to the policies stated in the SSA I-6 policy and procedures document by signing the document titled: "Agreement to Comply with the Orange County Social Services Agency Information Technology Security and Usage Policy" (Attachment V). This document also includes the SSA Confidentiality Agreement and serves as documentation of completion of the SSA Information Security Rules of the Road training presentation. This action must occur prior to a workforce member being provided with access to Confidential Information.

   Maintain this signed "Agreement to Comply with the Orange County Social Services Agency Information Technology Security and Usage Policy" (Attachment V) for three years after the non-County workforce member separates from SSA.

2. County of Orange Information Technology Usage Policy (Attachment I).

If this workforce member requires access to the SSA network or databases (e.g., shared drives, Statewide Eligibility Determination System, Imaging System, Child Welfare Services/Case Management System, SSA Intranet, etc.), a copy of the signed "Agreement to Comply with the Orange County Social Services Agency Information Technology Security and Usage Policy" (Attachment V) shall be provided to SSA's System Support Team and OCIT via the provisioning process. Network access will not be provided until this signed document is received.

V. ATTACHMENTS

VI. RELATED SSA POLICIES

1. P&P F21 Privacy and Security Incidents of Personally Identifying Information (PII) and Confidential Information

2. P&P D20: Remote Work

VII. REFERENCES

---

1. California Welfare and Institutions Code, Division 9, Part 2, Chapter 5

   1. 2. California Penal Code, Section 502

Attachment D

County of Orange Information Technology Security Provisions

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

1. County of Orange Information Technology Security Guidelines: County of Orange security standards follows the latest National Institute of Standards and Technology (NIST) 800-53 framework to ensure the highest levels of operational resiliency and cybersecurity.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

6. **General Security Guidelines:** Contractor will be solely responsible for the information technology infrastructure, including all computers, software, databases, electronic systems (including database management systems, email systems, auditing, and monitoring systems)

and networks used by or for Contractor ("Contractor Systems") to access County resources (including County systems), County data or otherwise in connection with the Services and shall prevent unauthorized access to County resources (including County systems) or County data through the Contractor Systems.

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

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

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

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

8. **Security Breach Notification:** In the event Contractor becomes aware of any act, error or omission, negligence, misconduct, or security incident including unsecure or improper data disposal, theft, loss, unauthorized use and disclosure or access, that compromises or is suspected to compromise the security, availability, confidentiality, and/or integrity of County data or the physical, technical, administrative, or organizational safeguards required under this

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

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

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

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

Notification shall be sent to:

Andrew Alipanah, MBA, CISSP	Linda Le, CHPC, CHC, CHP
Chief Information Security Officer	County Privacy Officer
1055 N. Main St., 6th Floor	1055 N. Main St., 6th Floor
Santa Ana, CA 92701	Santa Ana, CA 92701
Phone: (714) 567-7611	Phone: (714) 834-4082
Andrew.Alipanah@ocit.ocgov.com	Linda.Le@ocit.ocgov.com

County of Orange

Social Services Agency
Contracts Services
500 N. State College Blvd, Suite 100
Orange, CA 92868
714-541-7785
Karen.Vu@ssa.ocgov.com

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

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

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

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

10. **Business Continuity and Disaster Recovery (BCDR):**

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

The Contractor shall maintain a comprehensive risk management program focused on managing risks to County operations and data, including mitigation of the likelihood and impact of an adverse event occurring that would negatively affect contracted services and

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

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

Attachment E
State Privacy and Security Provisions

1. **DEFINITIONS**

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

   a. "**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.

   b. "**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.

   c. "**Contractor Staff**" means those employees of the contractor/subcontractor, 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.

   d. "**PII**" is personally identifiable information that is obtained through the MEDS or IEVS on behalf of the programs and can be used alone, or in conjunction with any other reasonably available information, to identify a specific individual. The Pll includes, but is not limited to, an individual's name, social security number, driver's license number, identification number, biometric records, date of birth, place of birth, or mother's maiden name. The Pll may be electronic, paper, verbal, or recorded.

   e. "**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 CalSAWS (California Statewide Welfare System), or under the control of a contractor, subcontractor or vendor of the county, on behalf of the county.

    f.   "Secure Areas" means any area where:

        i.   Contractor Staff assist in the administration of their program;

        ii.   Contractor Staff use or disclose Pll; or

        iii.   PII is stored in paper or electronic format.

2. PRIVACY AND CONFIDENTIALITY

    a.   The County staff, contractors, subcontractors and vendors, covered by this Agreement may use or disclose Pll 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, and Section 14100.2 of the Welfare and Institutions Code, Section 431.300 et. Seq. of Title 42 Code of Federal Regulations, or as authorized or required by law. Disclosures, which are authorized or required by law, such as a court order, or are made with the explicit written authorization of the individual, who is the subject of the PII, are allowable. Any other use or disclosure of Pll requires the express approval in writing by County of Orange. No Contractor Staff shall duplicate, disseminate or disclose Pll except as allowed in this Agreement.

    b.   Pursuant to this Agreement, Contractor Staff may only use PII to perform administrative functions related to administering their respective programs.

    c.   Access to Pll shall be restricted to Contractor Staff who need to perform their official duties to assist in the administration of their respective programs.

    d.   Contractor Staff who access, disclose or use Pll 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.

3. PERSONNEL CONTROLS

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

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

    i. Provide initial privacy and security awareness training to each new Contractor Staff within thirty (30) days of employment and;

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

    iii. Maintain records indicating each Contractor Staff's name and the date on which the privacy and security awareness training was completed;

    iv. Retain training records for a period of three (3) years after completion of the training.

b. **Employee Discipline**.

    i. Provide documented sanction policies and procedures for Contractor Staff who fail to comply with privacy policies and procedures or any provisions of these requirements.

    ii. Sanction policies and procedures shall include termination of employment when appropriate.

c. **Confidentiality Statement**. Ensure that all Contractor Staff, accessing, using or disclosing PII, sign a confidentiality statement (provided by the County). The statement shall be signed by Contractor staff 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.

The statement shall include at a minimum:

    i. General Use;

    ii. Security and Privacy Safeguards;

    iii. Unacceptable Use; and

    iv. Enforcement Policies.

d. **Background Screening**.

    i. Conduct a background screening of a Contractor Staff before they may access PII.

ii. 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.

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

4. 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 reviews of work activity by Contractor Staff, 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 must 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.

5. INFORMATION SECURITY AND PRIVACY STAFFING

The Contractor agrees to:

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

b. Provide County with applicable contact information for these designated individuals. Any changes to this information should be reported to County within ten (10) days.

c. Assign staff to be responsible for administration and monitoring of all security related controls stated in this Agreement.

6. PHYSICAL SECURITY

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

a. Secure all areas of the Contractor's facilities where Contractor Staff assist in the administration of their program and use, disclose, or store Pll.

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

    i. Properly coded key cards

    ii. Authorized door keys

    iii. Official identification

c. Issue identification badges to Contractor Staff.

d. Require Contractor Staff 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 Contractor facilities and leased facilities where five hundred (500) or more individually identifiable records of PII is used, disclosed or stored. Video surveillance 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 Contractor Staff. Visitors to the data center area must be escorted at all times by authorized Contractor Staff.

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 have multi-use 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 Contractor shall have policies that include, based on applicable risk factors, a description of the circumstances under which the Contractor Staff can transport PII, as well as the physical security requirements during transport. A Contractor that chooses to permit its staff to leave records unattended in vehicles must include provisions in its policies to ensure the PII is stored in a non-visible area such as a trunk, that the vehicle is locked, and under no circumstances permit PII be left unattended in a vehicle overnight or for other extended periods of time.

j. The Contractor shall have policies that indicate Contractor Staff are not to leave records with PII unattended at any time in airplanes, buses, trains, etc., including 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.

7. **TECHNICAL SECURITY CONTROLS**

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

   b. **Server Security**. Servers containing unencrypted PII must 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 data, must be encrypted when stored on any mobile device or removable media (i.e. USB drives, CD/DVD, smartphones, tablets, backup tapes etc.). Encryption must 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, must install and actively use an antivirus software solution. Antivirus software should have automatic updates for definitions scheduled at least daily.

f. **Patch Management**.

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

  ii. There must be a documented patch management process that determines installation timeframe based on risk assessment and vendor recommendations.

  iii. At a maximum, all applicable patches deemed as critical must 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.

  iv. Applications and systems that cannot be patched within this time frame, due to significant operational reasons, must have compensatory controls implemented to minimize risk.

g. **User IDs and Password Controls**.

  i. All users must be issued a unique username for accessing PII.

  ii. Username must be promptly disabled, deleted, or the password changed upon the transfer or termination of an employee within twenty-four (24) hours. Note: Twenty-four (24) hours is defined as one (1) working day.

  iii. Passwords are not to be shared.

  iv. Passwords must be at least eight (8) characters.

  v. Passwords must be a non-dictionary word.

  vi. Passwords must not be stored in readable format on the computer or server.

  vii. Passwords must be changed every ninety (90) days or less.

  viii. Passwords must be changed if revealed or compromised.

  ix. Passwords must be composed of characters from at least three (3) of the following four (4) 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. **Data Destruction**. When no longer needed, all PII must be cleared, purged, or destroyed consistent with NIST SP 800-88, Guidelines for Media Sanitization, such that the PII cannot be retrieved.

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

j. **Warning Banners**. The systems providing access to PII must display a warning banner stating, at a minimum:

    i. Data is confidential;

    ii. Systems are logged;

    iii. System use is for business purposes only, by authorized users; and

    iv. Users shall log off the system immediately if they do not agree with these requirements.

k. **System Logging**.

    i. The systems which provide access to PII must maintain an automated audit trail that can identify the user or system process which initiates a request for PII or alters PII.

    ii. 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.

    iii. If PII is stored in a database, database logging functionality shall be enabled.

    iv. Audit trail data shall be archived for at least three (3) years from the occurrence.

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

m. **Transmission Encryption**.

    i. All data transmissions of PII outside of a secure internal network must 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.

    ii. Encryption can be end to end at the network level, or the data files containing PII can be encrypted.

    iii. This requirement pertains to any type of PII in motion such as website access, file transfer, and email.

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

8. **AUDIT CONTROLS**

a. **System Security Review**.

    i. The Contractor must ensure audit control mechanisms are in place.

    ii. All systems processing and/or storing PII must 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.

    iii. Reviews should include vulnerability scanning tools.

b. **Log Reviews**. All systems processing and/or storing PII must 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 must 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 or DHCS suspects MEDS usage anomalies, the County will work with Contractor to investigate the anomalies and report

conclusions of such investigations and remediation to California Department of Social Services (CDSS).

9. BUSINESS CONTINUITY / DISASTER RECOVERY CONTROLS

a. **Emergency Mode Operation Plan**. The Contractor must 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.

b. **Data Centers**. Data centers with servers, data storage devices, and critical network infrastructure involved in the use, storage and/or processing of PII, must include environmental protection such as cooling, power, and fire prevention, detection, and suppression.

c. **Data Backup and Recovery Plan**.

   i. The Contractor shall have established documented procedures to backup PII to maintain retrievable exact copies of PII.

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

   iii. The procedures shall include storing backups offsite.

   iv. The procedures shall ensure an inventory of backup media.

   v. The Contractor shall have established documented procedures to recover PII data.

   vi. The documented recovery procedures shall include an estimate of the amount of time needed to restore the PII data.

   vii. It is recommended that the Contractor periodically test the data recovery process.

10. 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 Contractor shall have policies that include, based on applicable risk factors, a description of the circumstances under which the Contractor Staff can transport PII, as well as the physical security requirements during transport. A Contractor that chooses to permit its staff to leave records unattended in vehicles must include provisions in its policies to ensure the PII is stored in a non-visible area such as a trunk, that the vehicle is locked, and under no circumstances permit PII 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., including 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 must be disposed of through confidential means, such as cross-cut shredding or pulverizing.

f. **Removal of Data**. The PII must not be removed from the premises of Contractor except for identified routine business purposes or with express written permission of HHS.

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

h. **Mailing**.

    i.   Mailings containing PII shall be sealed and secured from damage or inappropriate viewing of PII to the extent possible.

    ii.   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 Contractor obtains prior written permission from HHS to use another method.

11. <u>NOTIFICATION AND INVESTIGATION OF BREACHES AND SECURITY INCIDENTS</u>

During the term of this Agreement, the County 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 HHS:

    i.   The Contractor will provide initial notice to the County. The Contractor agrees to perform the following incident reporting to County.

    ii.   Immediately upon discovery of a suspected security incident that involves data provided to Contractor by County, the Contractor will notify the County by email or telephone.

    iii.   Within one working day of discovery, the Contractor will notify the County by email or telephone of unsecured PII, if that PII was, or is, reasonably believed to have been accessed or acquired by an unauthorized person, any suspected security incident, intrusion, or unauthorized access, use, or disclosure of PII in violation of this Agreement, or potential loss of confidential data affecting this Agreement. Notice shall be made by contacting the County as provided in this agreement, including all information known at the time.

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

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

A. Prompt corrective action to mitigate any risks or damages involved with the breach and to protect the operating environment; and

B. Any action pertaining to such unauthorized disclosure required by applicable Federal and State laws and regulations.

b. Investigation and Investigative Report. The Contractor shall immediately investigate breaches and security incidents involving PII. The Contractor will cooperate with the County during this investigation. Within seventy-two (72) hours of discovery, the Contractor shall provide new or updated information if available to County. The updated report shall include any other applicable information related to the breach or security incident known at that time. The Contractor shall provide status update to County on a regular basis as agreed upon.

The Contractor shall provide to County all specific and pertinent information about the Breach, including copies of any reports conducted by the Contractor or on behalf of the Contractor. The Contractor shall waive any assertion of privilege in relation to such reports. Such information and/or reports shall be provided to County without unreasonable delay and in no event later than fifteen (15) calendar days the Contractor have such information and/or report.

c. **Complete Report**. 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 include a Corrective Action Plan (CAP) which includes, at a minimum, detailed information regarding the mitigation measures taken to halt and/or contain the improper use or disclosure.

If County requests additional information related to the incident, the Contractor shall make reasonable efforts to provide County with such information. County will review report and determine whether a breach occurred and whether individual

notification is required. County will maintain the final decision making over a breach determination.

d. **Notifications of Individuals**. When applicable state or federal law requires notification to individuals of a breach or unauthorized disclosure of their PII, the County will make the decision to either notify clients or have the Contractor give notice. If the Contractor shall give the notice, it would be subject to the following provisions:

    i.   If the cause of the breach is attributable to the Contractor or its subcontractors, agents or vendors, the Contractor shall pay any costs of such notifications, as well as any and all costs associated with the breach. If there are any questions as to whether the County or the Contractor is responsible for the breach, the County and the Contractor shall jointly determine responsibility for purposes of allocating the costs;

    ii.   All notifications (regardless of breach status) regarding the 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 the United States Code, inclusive of its implementing regulations, including but not limited to the requirement that the notifications be made without reasonable delay and in no event, later than sixty (60) calendar days from discovery;

    iii.   The County has contractual requirement with the California Department of Social Services and California Department of Health Care Services to approve the time, manner and content of any such notifications and their review and approval shall be obtained before notifications are made. Therefore, the Contractor must provide the notifications to County to obtain review and approval prior to notifications are made. If notifications are distributed without State review and approval, secondary follow-up notifications may be required; and

    iv.   The County may elect to assume responsibility for such notification from the Contractor.

e. **Responsibility for Reporting of Breaches when Required by State or Federal Law**. If the cause of a breach is attributable to the Contractor or its agents,

subcontractors or vendors, the Contractor is responsible for all required reporting of the breach. If the cause of the breach is attributable to the County, the County 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 (Department of Health Care Services) and COSS (California Department of Social Services) (if the breach involves MEDS or SSA data), then the Contractor shall coordinate with the County 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. **County Contact Information**. The Contractor shall 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 shall not require an amendment to this Agreement or any other agreement into which it is incorporated.

The preferred method of communication is email, when available. Do not include any Medi-Cal Pl/PII unless requested by County.

SSA Contract Analyst	County Privacy Officer

County of Orange
Social Services Agency
Contracts Services
500 N. State College Blvd,
Suite 100
Orange, CA 92868
 	
Attn: Contract Administrator
	Linda Le, CHC, CHPC, CHP
	County of Orange
	OCIT - Enterprise Privacy &
	Cybersecurity
	
	1055 N. Main St, 6th Floor
	Santa Ana, CA 92701
	
	Email: privacyofficer@ocgov.com
	    securityadmin@ocit.ocgov.com
	    linda.le@ocit.ocgov.com
	
	Telephone: (714) 834-4082

12. **COMPLIANCE WITH SSA (SOCIAL SECURITY ADMINISTRATION) AGREEMENT**

The County has agree 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 COSS, and in the Electronic Information Exchange Security Requirements and Procedures for State and Local Agencies Exchanging Electronic Information with SSA (TSSR). If Contractor have access to the PII data provided by SSA, then Contractor must agree to comply with the applicable privacy and security requirements, which is 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.

13. **COMPLIANCE WITH DEPARTMENT OF HOMELAND SECURITY AGREEMENT**

The County has agreed 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. If Contractor have access to the PII data provided by DHS-USCIS, then Contractor must agree to comply with the applicable privacy and security requirements, which is 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.

14. **CONTRACTOR AGENTS. SUBCONTRACTORS, AND VENDORS**

The Contractor agrees to enter into written agreements with all agents, subcontractors, and vendors that have access to the Contractor's PII. These agreements will impose, at a minimum, the same restrictions and conditions that apply to the Contractor with respect to PII upon such agents, subcontractors, and vendors. These shall include, 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 Contractor. If the agents, subcontractors, and vendors of the Contractor access data provided to the County by SSA or DHS-USCIS, the Contractor shall also incorporate the Agreement's Attachments into each subcontract or subaward with agents, subcontractors, and vendors.

15. **ASSESSMENTS AND REVIEWS**

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

16. **ASSISTANCE IN LITIGATION OR ADMINISTRATIVE PROCEEDINGS**

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

and any subcontractors, agents, and employees available to the Contractor at no cost to the Contractor to testify as witnesses, in the event of litigation or administrative proceedings involving the Contractor based upon claimed violations by the County of the privacy or security of PII, or state or federal laws or agreements concerning privacy or security of PII.