MEMORANDUM OF UNDERSTANDING

By and Between

California Department of Social Services

And

The County of Orange Social Services Agency

A. PURPOSE

This Memorandum of Understanding (MOU) is entered into by the California Department of Social Service (CDSS), and Orange County Social Services Agency (County) for the purpose of transferring administration of the County's CalFresh Restaurant Meals Program (RMP) to CDSS. This MOU allows participating RMP restaurant vendors to maintain program eligibility while the County's RMP is transferred to CDSS and until they execute a separate RMP restaurant vendor agreement with CDSS.

The CalFresh RMP is a program that provides the option for eligible persons and their spouses to use their CalFresh Food benefits to purchase prepared meals from approved participating RMP restaurant vendors within counties that have a RMP. Eligible persons generally include persons aged 60 or older, persons with disabilities and homeless persons.

In 2019, Welfare and Institutions Code 18919 was amended to allow for the creation of a statewide RMP to be administered by CDSS. Prior to that amendment, RMPs were administered only at the local level by participating counties.

Pursuant to All County Letter (ACL) No. 21-100, participating counties have the option of continuing to administer their local RMPs or transferring the administration of their RMPs to the CDSS.

Consistent with ACL No. 21-100, County has elected to transfer administration of its RMP to CDSS.

This MOU will govern the rights and responsibilities of the parties during the transfer of County's RMP to CDSS.

B. DATE OF TRANSFER OF COUNTY RMP

It is the intent of the parties that administration of County's RMP shall be transferred in its entirety, except as otherwise specified in this MOU, from County to CDSS on July 1, 2023. County agrees to cease entering into agreements with new RMP restaurant vendors on July 1, 2023. Any outstanding RMP restaurant

vendors whose applications with the United States Department of Agriculture, Food and Nutrition Services (USDA-FNS) are approved after July 1, 2023 must be given notice by County that they must enter into a separate agreement directly with CDSS to participate in the CDSS statewide RMP.

C. JOINT RESPONSIBILITIES

1. Pursuant to the terms and conditions set forth under this MOU, CDSS and the County agree to comply with all program related requirements up to and through the completion of transfer of administration of the RMP, in accordance with federal and/or state laws, policies, rules and regulations including, but not limited to: USDA-FNS regulations, USDA-FNS policy and information letters, CDSS information letters, and supplemental program documents.

2. Each Party shall respond in a timely manner to other's communications.

3. To the extent it is practical, the parties shall jointly prepare and County shall send a notification to participating RMP restaurant vendors advising of the date of the change of RMP administration, any new requirements for participation and the contact information for CDSS. Notification shall be transmitted as required in the County RMP agreement with the RMP restaurant vendor.

D. COUNTY RESPONSIBILITIES:

1. As soon as possible after the execution of this MOU, but no later than four weeks after this MOU has been executed, the County will provide CDSS with a list of its participating RMP restaurant vendors. The list shall include:

   a. RMP restaurant vendor name
   b. RMP restaurant vendor address
   c. Name and contact information of the individual for RMP restaurant vendor
   d. USDA-FNS RMP restaurant vendor ID number
   e. Month and year RMP restaurant vendor was approved by USDA-FNS to join the RMP

2. As soon as is practical after the execution of this MOU, the County shall transfer copies of all of its existing RMP files to CDSS by a means mutually agreeable to the parties.

3. The County shall advise CDSS of the status of any and all current complaints, investigations or other actions involving participating RMP restaurant vendors. The County shall continue to take all necessary action on any such matter until it has been successfully transferred to CDSS. If the matter may not be transferred to CDSS, the County shall prosecute the matter until a suitable resolution is obtained.

4. After transfer of administration of the RMP, County agrees to direct RMP inquiries to the CDSS Representative or another CDSS designated contact.

5. Contractor shall follow the requirements of the attached Exhibit E- Attachment 1 Confidentiality and Information Security Requirements Contractor/Entity v 2019 01.

E. CDSS Responsibilities

CDSS shall be responsible for the enrollment of new restaurant vendors as part of the RMP within County commencing with the date of transfer in B.

F. TERM:

The term of this MOU commences upon execution and shall remain in effect until amended by the parties or terminated by either party as described herein.

G. GENERAL PROVISIONS

This MOU may be modified or amended at any time by written mutual consent. Either party may terminate this MOU by giving thirty (30) days written notice to the other party.

This MOU is not effective until signed by both parties.

H. AUTHORIZED REPRESENTATIVES

The individuals below shall act as representatives of the parties during the term of this MOU. Either party may change its representative upon written notice to the other party. A change in representative shall not require a modification or amendment to the agreement.

CDSS		County	
Name	David Dye	Name	An Tran
Title	Statewide CalFresh RMP Manager	Title	Agency Director
Address	744 P Street Sacramento, CA 95814	Address	500 N. State College Blvd, Suite 100 Orange, CA 92868
Phone	916-247-6379	Phone	714-541-7773
Email	David.dye@dss.ca.gov	Email	an.tran@ssa.ocgov.com

THE PARTIES HERETO have executed this MOU:

The persons executing this MOU on behalf of their respective parties hereby represent and warrant that they have the right, power, legal capacity, and appropriate authority to execute this MOU on behalf of the party for which they sign.

County	CDSS
An Tran	
Name	Name
Agency Director	
Title	Title
Signature	Signature
Date	Date

APPROVED AS TO FORM
COUNTY COUNSEL
COUNTY OF ORANGE, CALIFORNIA

Carolyn S. Frost	Senior Deputy County Counsel
Print Name	Title
DocuSigned by: Carolyn S. Frost D3AB98D76D0B425...	3/30/2023 | 9:09:43 AM PDT
Signature	Date

The California Department of Social Services
Confidentiality and Information Security Requirements
Contractor/Entity - v 2019 01

This Confidentiality and Information Security Requirements Exhibit (hereinafter referred to as "this Exhibit") sets forth the information security and privacy requirements Contractor/Entity (hereinafter referred to as "Contractor") is obligated to follow with respect to all confidential and sensitive information (as defined herein) disclosed to or collected by Contractor, pursuant to Contractor's Agreement (the "Agreement") with the California Department of Social Services (hereinafter "CDSS") in which this Exhibit is incorporated. The CDSS and Contractor desire to protect the privacy and provide for the security of CDSS Confidential, Sensitive, and/or Personal (CSP) Information (hereinafter referred to as "CDSS CSP") in compliance with state and federal statutes, rules and regulations.

I. **Order of Precedence.** With respect to information security and privacy requirements for all CDSS CSP, unless specifically exempted, the terms and conditions of this Exhibit shall take precedence over any conflicting terms or conditions set forth in any other part of the Agreement between Contractor and CDSS.

II. **Effect on lower tier transactions.** The terms of this Exhibit shall apply to all lower tier transactions (e.g. agreements, sub-agreements, contracts, subcontracts, and sub-awards, etc.). Contractor shall incorporate the contents of this Exhibit into each lower tier transaction.

III. **Confidentiality of Information.**

a. **DEFINITIONS**. The following definitions apply to this Exhibit and relate to CDSS Confidential, Sensitive, and/or Personal Information.

i. "Confidential Information" is information maintained by the CDSS that is exempt from disclosure under the provisions of the California Public Records Act (Government Codes Sections 6250 et seq.) or has restrictions on disclosure in accordance with other applicable state or federal laws.

ii. "Sensitive Information" is information maintained by the CDSS, which is not confidential by definition, but requires special precautions to protect it from unauthorized access and/or modification (i.e., financial or operational information). Sensitive information is information in which the disclosure would jeopardize the integrity of the CDSS (i.e., CDSS' fiscal resources and operations).

iii. "Personal Information" is information, in any medium (paper, electronic, or oral) that identifies or describes an individual (i.e., name, social security number, driver's license, home/mailing address, telephone number, financial matters with security codes, medical insurance policy number, Protected Health Information (PHI), etc.) and must be protected from inappropriate access, use or disclosure and must be made accessible to information subjects upon request. It can also be information in the possession of the Department in which the disclosure is limited by law or contractual Agreement (i.e., proprietary information, etc.).

iv. "Breach" is

1. the unauthorized acquisition, access, use, or disclosure of CDSS CSP in a manner which compromises the security, confidentiality or integrity of the information; or

2. the same as the definition of "breach of the security of the system" set forth in California Civil Code section 1798.29(f).

v. “Information Security Incident” is

1. unauthorized access or disclosure, modification or destruction of, or interference with, CDSS CSP that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of any state or federal law or in a manner not permitted under the Agreement between Contractor and CDSS, including this Exhibit.

b. CDSS CSP which may become available to Contractor as a result of the implementation of the Agreement shall be protected by Contractor from unauthorized access, use, and disclosure as described in this Exhibit.

c. Contractor is notified that unauthorized disclosure of CDSS CSP may be subject to civil and/or criminal penalties under state and federal law, including but not limited to:

- California Welfare and Institutions Code section 10850
- Information Practices Act - California Civil Code section 1798 et seq.
- Public Records Act - California Government Code section 6250 et seq.
- California Penal Code Section 502, 11140-11144, 13301-13303
- Health Insurance Portability and Accountability Act of 1996 (“HIPAA”) - 45 CFR Parts 160 and 164
- Safeguarding Information for the Financial Assistance Programs - 45 CFR Part 205.50
- Unemployment Insurance Code section 14013

d. **EXCLUSIONS.** “Confidential Information”, “Sensitive Information”, and “Personal Information” (CDSS CSP) does not include information that

i. is or becomes generally known or available to the public other than because of a breach by Contractor of these confidentiality provisions;

ii. already known to Contractor before receipt from CDSS without an obligation of confidentiality owed to CDSS;

iii. provided to Contractor from a third party except where Contractor knows, or reasonably should know, that the disclosure constitutes a breach of confidentiality or a wrongful or tortious act; or

iv. independently developed by Contractor without reference to the CDSS CSP.

IV. Contractor Responsibilities.

a. **Training.** Contractor shall instruct all employees, agents, and subcontractors with access to the CDSS CSP regarding:

i. The confidential nature of the information;

ii. The civil and criminal sanctions against unauthorized access, use, or disclosure found in the California Civil Code Section 1798.55, Penal Code Section 502 and other state and federal laws;

iii. CDSS procedures for reporting actual or suspected information security incidents in Paragraph V - Information Security Incidents and/or Breaches; and

iv. That unauthorized access, use, or disclosure of CDSS CSP is grounds for immediate termination of this Agreement with CDSS and Contractor and may be subject to penalties, both civil and criminal.

b. Use Restrictions. Contractor shall take the appropriate steps to ensure that their employees, agents, and subcontractors will not intentionally seek out, read, use, or disclose the CDSS CSP other than for the purposes described in the Agreement and to meet its obligations under the Agreement.

c. Disclosure of CDSS CSP. Contractor shall not disclose any individually identifiable CDSS CSP to any person other than for the purposes described in the Agreement and to meet its obligations under the Agreement.

d. Subpoena. If Contractor receives a subpoena or other validly issued administrative or judicial notice requesting the disclosure of CDSS CSP, Contractor will immediately notify the CDSS Program Contract Manager and the CDSS Information Security and Privacy Officer. In no event should notification to CDSS occur more than three (3) business days after receipt by Contractor's responsible unit for handling subpoenas and court orders.

e. Information Security Officer. Contractor shall designate an Information Security Officer to oversee its compliance with this Exhibit and to communicate with CDSS on matters concerning this Exhibit.

f. Requests for CDSS CSP by Third Parties. Contractor shall promptly transmit to the CDSS Program Contract Manager and the CDSS Information Security and Privacy Officer all requests for disclosure of any CDSS CSP requested by third parties to the Agreement between Contractor and CDSS (except from an Individual for an accounting of disclosures of the individual's personal information pursuant to applicable state or federal law), unless prohibited from doing so by applicable state or federal law.

g. Documentation of Disclosures for Requests for Accounting. Contractor shall maintain an accurate accounting of all requests for disclosure of CDSS CSP Information and the information necessary to respond to a request for an accounting of disclosures of personal information as required by Civil Code section 1798.25, or any applicable state or federal law.

h. **Return or Destruction of CDSS CSP on Expiration or Termination**. Upon expiration or termination of the Agreement between Contractor and CDSS, or upon a date mutually agreed upon by the Parties following expiration or termination, Contractor shall return or destroy the CDSS CSP. If return or destruction is not feasible, Contractor shall provide a written explanation to the CDSS Program Contract Manager and the CDSS Information Security and Privacy Officer, using the contact information in this Agreement. CDSS, in its sole discretion, will make a determination of the acceptability of the explanation and, if retention is permitted, shall inform Contractor in writing of any additional terms and conditions applicable to the retention of the CDSS CSP.

i. **Retention Required by Law.** If required by state or federal law, Contractor may retain, after expiration or termination, CDSS CSP for the time specified as necessary to comply with the law.

j. **Obligations Continue Until Return or Destruction**. Contractor's obligations regarding the confidentiality of CDSS CSP set forth in this Agreement, including but not limited to obligations related to responding to Public Records Act requests and subpoenas shall continue until Contractor returns or destroys the CDSS CSP or returns the CDSS CSP to CDSS; provided however, that on expiration or termination of the Agreement between Contractor and CDSS, Contractor shall not further use or disclose the CDSS CSP except as required by state or federal law.

k. **Notification of Election to Destroy CDSS CSP**. If Contractor elects to destroy the CDSS CSP, Contractor shall certify in writing, to the CDSS Program Contract Manager and the CDSS Information Security and Privacy Officer, using the contact information, that the CDSS CSP has been destroyed.

l. **Background Check.** Before a member of Contractor's workforce may access CDSS CSP, Contractor must conduct a thorough background check of that worker and evaluate the results to assure that there is no indication that the worker may present a risk to CDSS information technology systems and/or CDSS data. Contractor shall retain each workforce member's background check documentation for a period of three (3) years following Agreement termination.

m. **Confidentiality Safeguards.** Contractor shall implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the CDSS CSP that it creates, receives, maintains, uses, or transmits pursuant to the Agreement. Contractor shall develop and maintain a written information privacy and security program that includes administrative, technical and physical safeguards appropriate to the size and complexity of Contractor's operations and the nature and scope of its activities, including at a minimum the following safeguards:

    i. **General Security Controls**

        1. **Confidentiality Acknowledgement.** By executing this Agreement and signing Paragraph XI, CDSS Confidentiality and Security Compliance Statement, Contractor acknowledges that the information resources maintained by CDSS and provided to Contractor may be confidential, sensitive, and/or personal and requires special precautions to protect it from wrongful access, use, disclosure, modification, and destruction.

2. **Workstation/Laptop Encryption.** All Contractor-owned or managed workstations, laptops, tablets, smart phones, and similar devices that process and/or store CDSS CSP must be encrypted using a FIPS 140-2 certified algorithm which is 128 bit or higher, such as Advanced Encryption Standard (AES). The encryption solution must be full disk unless approved by the CDSS Information Security Office.
3. **Data Encryption.** Any CDSS CSP shall be encrypted at rest when stored on network file shares or document repositories.
4. **Server Security.** Servers containing unencrypted CDSS CSP must have sufficient administrative, physical, and technical controls in place to protect that data, based upon a risk assessment/system security review.
5. **Minimum Necessary.** Only the minimum necessary amount of the CDSS CSP required to perform necessary business functions may be copied, downloaded, or exported.
6. **Removable Media Devices.** All electronic files that contain the CDSS CSP must be encrypted when stored on any removable media or portable device (i.e. USB thumb drives, floppies, CD/DVD, smart phone, backup tapes etc.). Encryption must be a FIPS 140-2 certified algorithm which is 128 bit or higher, such as AES.
7. **Antivirus Software.** All Contractor-owned or managed workstations, laptops, tablets, smart phones, and similar devices that process and/or store CDSS CSP must install and actively use comprehensive anti-virus software solution with automatic updates scheduled at least daily.
8. **Patch Management.** To correct known security vulnerabilities, Contractor shall install security patches and updates in a timely manner on all Contractor-owned or managed workstations, laptops, tablets, smart phones, and similar devices that process and/or store CDSS CSP as appropriate based on Contractor's risk assessment of such patches and updates, the technical requirements of Contractor's systems, and the vendor's written recommendations. If patches and updates cannot be applied in a timely manner due to hardware or software constraints, mitigating controls will be implemented based upon the results of a risk assessment.
9. **User IDs and Password Controls.** All users must be issued a unique user name for accessing CDSS CSP. Contractor's password policy must be based on information security best practices for password length, complexity, and reuse.
10. **Data Destruction.** Upon termination of the Agreement, all CDSS CSP must be sanitized in accordance with NIST Special Publication 800-88, Guidelines for Media Sanitization.

ii. **System Security Controls**

1. **System Timeout.** The system providing access to the CDSS CSP must provide an automatic timeout, requiring re-authentication of the user session after no more than thirty (30) minutes of inactivity for applications, and fifteen (15) minutes of inactivity for desktops and laptops.
2. **Warning Banners.** All systems (servers, desktops, laptops, etc.) containing CDSS CSP must display a warning banner at login stating that data is confidential, systems are logged, and system use is for business purposes only. User must be directed to log off the system if they do not agree with these requirements.
3. **System Logging.** The system must maintain an automated audit trail which can identify the user or system process which initiates a request for CDSS CSP, or which alters CDSS CSP. The audit trail must be date and time stamped, must log both successful and failed accesses, must be read only, and must be restricted to authorized users. If CDSS CSP is stored in a database, database logging functionality must be enabled. Audit trail data must be archived for at least one (1) year after occurrence.
4. **Access Controls.** The system must use role based access controls for all user authentications, enforcing the principle of least privilege.
5. **Transmission Encryption.** All data transmissions of CDSS CSP by Contractor outside the secure internal network must be encrypted using a FIPS 140-2 certified algorithm, such as Advanced Encryption Standard (AES), with a 128bit key or higher. Encryption can be end to end at the network level, or the data files containing CDSS CSP can be encrypted. This requirement pertains to any type of CDSS CSP in motion such as website access, file transfer, and email.
6. **Intrusion Detection**. All systems involved in accessing, holding, transporting, and protecting CDSS CSP that are accessible via the Internet must be protected by a comprehensive intrusion detection and prevention solution.

iii. **Audit Controls**

1. **System Security Review.** All systems processing and/or storing CDSS CSP must have at least an annual system risk assessment/security review which provides assurance that administrative, physical, and technical controls are functioning effectively and providing adequate levels of protection. Reviews shall include vulnerability scanning tools.
2. **Log Reviews.** All systems processing and/or storing CDSS CSP must have a routine procedure in place to review system logs for unauthorized access.

3. **Change Control.** All systems processing and/or storing CDSS CSP must have a documented change control procedure that ensures separation of duties and protects the confidentiality, integrity and availability of data.

iv. **Business Continuity / Disaster Recovery Controls**

1. **Disaster Recovery.** Contractor must establish a documented plan to enable continuation of critical business processes and protection of the security of electronic CDSS CSP 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.
2. **Data Backup Plan.** Contractor must have established documented procedures to backup CDSS CSP to maintain retrievable exact copies of CDSS CSP. The plan must include a regular schedule for making backups, storing backups offsite, an inventory of backup media, and the amount of time to restore CDSS CSP should it be lost. At a minimum, the schedule must be a weekly full backup and monthly offsite storage of CDSS data.

v. **Paper Document Controls**

1. **Supervision of Information**. CDSS CSP 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. CDSS CSP in paper form shall not be left unattended at any time in vehicles or planes and shall not be checked in baggage on commercial airplanes.
2. **Escorting Visitors**. Visitors to areas where the CDSS CSP are contained shall be escorted and CDSS CSP shall be kept out of sight while visitors are in the area.
3. **Confidential Destruction**. CDSS CSP must be disposed of through confidential means, such as cross cut shredding and/or pulverizing.
4. **Removal of Information**. CDSS CSP must not be removed from the premises of Contractor except for identified routine business purposes or with express written permission of CDSS.
5. **Faxing**. CDSS CSP that must be transmitted by fax shall require that Contractor confirms the recipient fax number before sending, takes precautions to ensure that the fax was appropriately received, maintains procedures to notify recipients if Contractor's fax number changes, and maintains fax machines in a secure area**.**
6. **Mailing**. Paper copies of CDSS CSP shall be mailed using a secure, bonded mail service, such as Federal Express, UPS, or by registered U.S. Postal Service (i.e., accountable mail using restricted delivery). All packages must be double packed with a sealed envelope and a sealed outer envelope or locked box.

V. Information Security Incidents and/or Breaches of CDSS CSP

a. **CDSS CSP Information Security Incidents and/or Breaches Response Responsibility**. The Contractor shall be responsible for facilitating the Information Security Incident and/or Breach response process as described in California Civil Code 1798.82(f), and State Administrative Manual (SAM) Section 5340, Information Security Incident Management, including, but not limited to, taking:

   i. Prompt corrective action to mitigate the risks or damages involved with the Information Security Incident and/or Breach and to protect the operating environment; and

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

b. **Discovery and Notification of Information Security Incidents and/or Breaches of CDSS CSP**. Contractor shall notify the CDSS Program Contract Manager and the CDSS Information Security and Privacy Officer of an Information Security Incident and/or Breach as expeditiously as practicable and without unreasonable delay, taking into account the time necessary to allow Contractor to determine the scope of the Information Security Incident and/or Breach, but no later than three (3) calendar days after the discovery of an Information Security Incident and/or Breach. Notification is to be made by telephone call and email.

c. **Isolation of System or Device.** A system or device containing CDSS CSP compromised by an exploitation of a technical vulnerability shall be promptly disconnected or quarantined and investigated until the vulnerability is resolved. Contractor will notify CDSS CSP within two (2) business days of a confirmed exploitation of a technical vulnerability and keep CDSS informed as to the investigation until resolution of the vulnerability is completed.

d. **Investigation of Information Security Incidents and/or Breaches**. Contractor shall promptly investigate Information Security Incidents and/or Breaches of CDSS CSP. CDSS shall have the right to participate in the investigation of such Information Security Incidents and/or Breaches. CDSS shall also have the right to conduct its own independent investigation, and Contractor shall cooperate fully in such investigations. Contractor is not required to disclose their un-redacted confidential, proprietary, or privileged information. Contractor will keep CDSS fully informed of the results of any such investigation.

e. **Updates on Investigation**. Contractor shall provide regular (at least once a week) email updates on the progress of the Information Security Incident and/or Breach investigation of CDSS CSP to the CDSS Program Contract Manager and the CDSS Information Security and Privacy Officer until the updates are no longer needed, as mutually agreed upon between Contractor and the CDSS Information Security and Privacy Officer. Contractor is not required to disclose their un-redacted confidential, proprietary, or privileged information.

f. **Written Report**. Contractor shall provide a written report of the investigation to the CDSS Program Contract Manager and the CDSS Information Security and Privacy Officer within thirty (30) business days of the discovery of the Information Security Incident and/or Breach of CDSS CSP. Contractor is not required to disclose their un-redacted confidential, proprietary, or privileged information. The report shall include, but not be limited to, if known, the following:

i. Contractor point of contact information;

ii. A description of what happened, including the date of the Information Security Incident and/or Breach of CDSS CSP and the date of the discovery of the Information Security Incident and/or Breach, if known;

iii. A description of the types of CDSS CSP that were involved and the extent of the information involved in the Information Security Incident and/or Breach;

iv. A description of the unauthorized persons known or reasonably believed to have improperly used or disclosed CDSS CSP;

v. A description of where the CDSS CSP is believed to have been improperly transmitted, sent, or utilized;

vi. A description of the probable causes of the improper use or disclosure;

vii. Whether Civil Code sections 1798.29 or 1798.82 or any other federal or state laws requiring individual notifications of breaches are triggered; and

viii. A full, detailed corrective action plan, including information on measures that were taken to halt and/or contain the Information Security Incident and/or Breach of CDSS CSP.

g. Cost of Investigation and Remediation. Per SAM Section 5305.8, Contractor shall be responsible for all direct and reasonable costs incurred by CDSS due to Information Security Incidents and/or Breaches of CDSS CSP resulting from Contractor's failure to perform or from negligent acts of its personnel, and resulting in the unauthorized disclosure, release, access, review, or destruction; or loss, theft or misuse of an information asset. These costs include, but are not limited to, notice and credit monitoring for twelve (12) months for impacted individuals, CDSS staff time, material costs, postage, media announcements, and other identifiable costs associated with the Information Security Incident, Breach and/or loss of data.

VI. Contact Information. To direct communications to the above referenced CDSS staff, Contractor shall initiate contact as indicated herein. CDSS reserves the right to make changes to the contact information below by giving written notice to Contractor. Said changes shall not require an amendment to this Exhibit or the Agreement to which it is incorporated.

CDSS Program Contract Manager	**CDSS Information Security & Privacy Officer**
See the Scope of Work exhibit for Program Contract Manager information	California Department of Social Services Information Security & Privacy Officer 744 P Street, MS 9-9-70 Sacramento, CA 95814 Email: iso@dss.ca.gov Telephone: (916) 651-5558

VII. **Audits and Inspections.** CDSS may inspect and/or monitor compliance with the safeguards required in this Exhibit. Contractor shall promptly remedy any violation of any provision of this Exhibit and shall certify the same to the CDSS Program Contract Manager and the CDSS Information Security and Privacy Officer in writing. The fact that CDSS inspects, or fails to inspect, or has the right to inspect, does not relieve Contractor of its responsibility to comply with this Exhibit.

VIII. **Amendment**. The parties acknowledge that federal and state laws regarding information security and privacy rapidly evolves and that amendment of this Exhibit may be required to provide for procedures to ensure compliance with such laws. The parties specifically agree to take such action as is necessary to implement new standards and requirements imposed by regulations and other applicable laws relating to the security or privacy of CDSS CSP.

IX. **Interpretation**. The terms and conditions in this Exhibit shall be interpreted as broadly as necessary to implement and comply with regulations and applicable State laws. The parties agree that any ambiguity in the terms and conditions of this Exhibit shall be resolved in favor of a meaning that complies and is consistent with federal and state laws and regulations.

X. **Termination.** An Information Security Incident and/or Breach of CDSS CSP by Contractor, its employees, agents, or subcontractors, as determined by CDSS, may constitute a material breach of the Agreement between Contractor and CDSS and grounds for immediate termination of the Agreement.

XI. CDSS Confidentiality and Security Compliance Statement

CALIFORNIA DEPARTMENT of SOCIAL SERVICES
CONFIDENTIALITY AND SECURITY COMPLIANCE STATEMENT v 2019 01

Information resources maintained by the California Department of Social Services (CDSS) and provided to Contractor may be confidential, sensitive, and/or personal and requires special precautions to protect it from wrongful access, use, disclosure, modification, and destruction.

We hereby acknowledge that the confidential and/or sensitive records of the CDSS are subject to strict confidentiality requirements imposed by state and federal law, which may include, but are not limited to, the following; the California Welfare and Institutions Code §10850, Information Practices Act - California Civil Code §1798 et seq., Public Records Act - California Government Code §6250 et seq., California Penal Code §502, 11140-11144, 13301-13303, Health Insurance Portability and Accountability Act of 1996 ("HIPAA") - 45 CFR Parts 160 and 164, and Safeguarding Information for the Financial Assistance Programs - 45 CFR Part 205.50. Contractor agrees to comply with the laws applicable to the CDSS CSP received.

This Confidentiality and Security Compliance Statement must be signed and returned with the Contract.

Project Representative

Name (Printed): _____

Title: _____

Business Name: _____

Email Address: _____

Phone: _____

Signature: _____

Date Signed: _____

READ and ACKNOWLEDGED: Information Security Officer (or authorized official responsible for business' information security program)

Name (Printed): _____

Title: _____

Business Name: _____

Email Address: _____

Phone: _____

Signature: _____

Date Signed: _____