MEMORANDUM OF UNDERSTANDING
BETWEEN
THE CALIFORNIA AUTOMATED CONSORTIUM ELIGIBILITY SYSTEM
AND
CALIFORNIA DEPARTMENT OF SOCIAL SERVICES

This MEMORANDUM OF UNDERSTANDING (MOU) is entered into by and between the State of California Department of Social Services (CDSS) and the California Automated Consortium Eligibility System (CalACES). CDSS and CalACES each may be referred to herein individually as a Party and collectively as Parties.

I. PURPOSE

The purpose of this MOU is to set forth the terms and conditions for CalACES to provide to CDSS necessary and relevant county Supplemental Nutrition Assistance Program (SNAP) recipient data retained by CalACES. The data to be provided to CDSS is needed to further California's participation in the U.S. Department of Agriculture, Food and Nutrition Service (FNS) SNAP Barriers Study (herein after referred to as the "Study"). The Study will identify the major individual, household, and environmental barriers affecting SNAP households' perceived ability to have access to a healthy diet throughout the month, examine how these barriers vary by household demographics, economics, and geography (urban/rural and FNS Regions) and determine how, if at all, these barriers can be accounted for in determining SNAP allotments.

II. BACKGROUND AND AUTHORITY

1. The CDSS is the single state agency responsible for the oversight and overall administration of the SNAP program (known in the State of California as CalFresh).

2. The CalFresh program is administered by the county welfare departments (CWDs) in the 58 counties in the State of California. The CWDs maintain application and case record data of CalFresh applicants and recipients (client data).

3. CalACES establishes itself as a Joint Powers Authority (JPA) by agreement with 40 of the 58 CWDs that provide a single legal entity for purposes of managing the C-IV and LRS Systems that maintains the client data of the applicable counties. The client data is confidential data as specified in Welfare and Institutions Code Section 10850 and required to be protected from unauthorized access in accordance with state and federal laws.

4. The WIC Section 10850 specifically authorizes any CWD in the state to provide "... lists of applicants for, or recipients of, public social services, to any other county welfare department or the State Department of Social Services, and these lists or any other records shall be released when requested by ...the State Department of Social Services. These ... records shall only be used for purposes directly connected with the administration of public social services," which is the case in this MOU.

5. The FNS authority for this initiative is 7 U.S.C. §2020(e)(8) which permits the disclosure of information obtained from applicant households to persons directly connected with the administration or enforcement of the provisions of SNAP, regulations issued pursuant to SNAP, federal assistance programs, or federally-assisted state programs. See also federal regulations at 7 C.F.R. 272.1(c)(i).

6. The FNS has contracted with Westat with its subcontractor, Insight Policy Research (contract number AG-3198-D-14-0071) to conduct the Study. Westat will draw a nationally representative sample and conduct a survey of approximately 4,800 SNAP participants from 30 States including California. From the completed SNAP surveys returned, Westat will select 120 individuals who will be invited to participate in an in-depth qualitative interview. Insight Policy Research will only be provided with the names and contact information for respondents who are selected for in-depth qualitative interviews based on their responses to the SNAP survey.

7. In order for Westat to draw the sample and contact respondents, Westat will need specific SNAP (CalFresh) benefit data elements held by the consortium and identified in Exhibit A.

III. SCOPE OF WORK

The CalACES agrees to provide to CDSS requested and available records of all CalFresh recipients specified in Exhibit A. CDSS will provide those records to Westat (pursuant to CDSS Data Use Agreement 17-6084) for purposes of conducting the SNAP Barriers Study as described in FNS contract number AG-3198-D-14-0071.

IV. CalACES RESPONSIBILITIES

1. CalACES agrees to use its best efforts to extract and send to CDSS the client data specified in Exhibit A using secure file transfer protocols and encryption that meet or exceed the standards described in Exhibit B, Confidentiality and Information Security Requirements.

2. CalACES agrees to work cooperatively with CDSS, if needed, in providing clarification of the client data sent to CDSS pursuant to Exhibit A.

3. As soon as feasible after the execution of this MOU, CalACES agrees to securely transmit to CDSS the client data specified in Exhibit A.

V. CDSS RESPONSIBILITIES

The CDSS, upon receipt of client data from CalACES, agrees to protect the confidentiality and security of the information in accordance with CDSS policies, procedures, and federal and state law applicable to public assistance programs, including but not limited to Welfare and Institutions Code Section 10850, and the California Information Practices Act commencing at Civil Code Section 1798.

CDSS shall require Westat to comply with the Confidentiality and Information Security Requirements set forth in Exhibit B attached hereto and applicable state and federal laws.

VI. TERM

This MOU shall be effective upon the signing of the authorized representatives of CDSS and CalACES. The MOU shall expire on July 29, 2020, unless terminated pursuant to Section IX, paragraph 2 below.

VII. FUNDING

There is no funding or fiscal reimbursement for the provision of the client data pursuant to this MOU.

VIII. CONTACTS

1. The following CDSS representative is authorized to implement the terms and conditions of the MOU and will be responsible for the oversight and supervision of the security and confidentiality of the client data sent to CDSS by CalACES:

Dionne Evans-Dean, Chief
Performance Monitoring and Research Bureau
California Department of Social Services
744 P St. MS 9-13-56
Sacramento, CA 95814
(916) 653-1430
dionne.evans-dean@dss.ca.gov

The CDSS will immediately notify CalACES, in writing, of a change of the contact person.

2. The following CDSS representative will serve as the sole point of contact (POC) for communication between CDSS and CalACES:

Jenny Chi, Staff Services Manager I
Performance Monitoring and Research Bureau
California Department of Social Services
744 P St. MS 9-13-56
Sacramento, CA 95814
(916) 653-1428
jenny.chi@dss.ca.gov

The CDSS will provide a five (5) day advance written notice to the CalACES for a change of the contact person for CDSS. CDSS will identify a designee to act on behalf of the POC in the event that the POC is unavailable.

3. The following CalACES representative will serve as the sole POC for communication between CalACES and CDSS:

Karen Rapponotti, CalACES North Deputy Director
CalACES
11290 Pyrites Way, Suite 150
Gold River, CA 95670
(916) 851-3208
rapponottikj@c-iv.org

The CalACES will provide a five (5) day advance notice to CDSS for a change of the contact person for CalACES. CalACES will identify a designee to act on behalf of the POC in the event that the POC is unavailable.

Either party may make changes to the contacts for this MOU. Said changes shall not require an amendment to this MOU.

IX. GENERAL PROVISIONS

1. AMENDMENTS. This MOU may be amended at any time by written mutual consent of the parties.

2. TERMINATION.

   a. Termination without cause: This MOU may be terminated by either party without cause upon 30 days' written notice.

b. Termination with cause. This MOU may be terminated immediately by either party if the terms of this MOU are violated in any manner.

c. Other grounds for termination. In the event that any other contract, agreement or MOU which is identified in Section II. Background, above, as being related to or necessary for the performance of this MOU, terminates or expires, this MOU may be terminated upon the effective date of the termination of that contract, agreement or MOU, even if such termination will occur with less than thirty (30) days written notice.

3. DISPUTE RESOLUTION PROCESS. If a dispute arises between CDSS and CalACES, CalACES must seek resolution using the process outline below:

CalACES should first informally discuss the problem with the CDSS program contact. If the problem cannot be resolved informally, CalACES must direct the grievance, in writing, to the CDSS program supervisor. The supervisor must make a decision within ten (10) working days after receipt of the written grievance from CalACES. Should CalACES disagree with the supervisor, CalACES may appeal to the appropriate CDSS upper management staff. The decision of the upper management staff of CDSS shall be the final decision.

X. AUTHORIZED REPRESENTATIVES

By signing below, the individual certifies that it is acting as the representative of the party identified below and possesses the authority to enter into this MOU on behalf of that party and that the party possesses the legal authority to enter into this MOU.

For CALIFORNIA DEPARTMENT OF SOCIAL SERVICES

Michael White, Staff Services Manager I
Contracts and Purchasing Bureau
California Department of Social Services
744 P Street, MS 8-14-747
Sacramento, CA 95814
michael.white@dss.ca.gov

Signature: _____ **Date:** _____
Michael White, Staff Services Manager I
Contracts and Purchasing Bureau

For CalACES

Scott Pettygrove, Chair, CalACES
2115 W. Wardrobe Avenue
P.O. Box 112
Merced, CA 95341-0112
(209) 385-3000 x 1-5300
spettygrove@hsa.co.merced.ca.us

John Boule, CalACES Executive Director
11290 Pyrites Way Suite 150
Rancho Cordova, CA 95670
(916) 851-3201
BouleJ@CalACES.org

Signature: _____ **Date:** _____
Scott Pettygrove, Chair, CalACES

Signature: _____ **Date:** _____
John Boule, CalACES Executive Director

Approved as to legal form:

Signature: _____ **Date:** _____
Phebe W. Chu, CalACES Legal Counsel

Exhibit A: Data Elements

Data from the administration of SNAP (CalFresh) from all households receiving SNAP benefits as of October 31, 2017 will include:

1) Contact information for the head of household for all households receiving SNAP benefits as of 10/31/17, including:

County Identification Number (CIN)	Name of head of household	All available addresses	All available telephone numbers

   a. CalACES will provide CIN and Personally Identifying Information to CDSS for all households.
   b. CDSS will transmit to Westat an initial dataset containing a unique identifier generated from the CIN and non-personally identifiable information (items 2 through 6 identified below).
   c. Upon randomization by Westat, CDSS will provide the name of head of household, all available addresses, and telephone numbers for individuals identified in the randomized sample.

2) Household size (total number of people included on case file).

3) Total number of children under 18 in household.

4) Latest uninterrupted benefit start date.

5) SNAP benefit payment date/transmission date.

6) Amount of monthly SNAP benefit.

The California Department of Social Services
Confidentiality and Information Security Requirements

Contractor/Entity - v 2017 10

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 and shall prevail over any such conflicting terms or conditions.

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.) regardless of whether they are for the acquisition of services, goods, or commodities. The Contractor shall incorporate the contents of this Exhibit into each lower tier transaction to its agents, contractors, subcontractors, or independent consultants, etc.

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. an attempted breach;
2. the attempted or successful unauthorized access or disclosure, modification or destruction of CDSS CSP, in violation of any state or federal law or in a manner not permitted under the Agreement between Contractor and CDSS, including this Exhibit; or
3. the attempted or successful modification or destruction of, or interference with, Contractor's system operations in an information technology system, that negatively impacts the confidentiality, availability or integrity of CDSS CSP.

b. CDSS CSP by the CDSS which may become available to the Contractor as a result of the implementation of the Agreement shall be protected by the 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

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. The 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 the Contractor and may be subject to penalties, both civil and criminal.

b. Use Restrictions. The Contractor shall take the appropriate steps to ensure that their employees, agents, contractors, subcontractors, and independent consultants will not intentionally seek out, read, use, or disclose the CDSS CSP other than for the purposes of providing the requested services to CDSS and meeting its obligations under the Agreement.

c. Disclosure of CDSS CSP. The Contractor shall not disclose any individually identifiable CDSS CSP to any person other than for the purposes of providing the requested services to CDSS and meeting its obligations under the Agreement. Contractor is permitted to disclose individually identifiable CDSS CSP with the consent of the individual to its service providers, its vendors, and its partners for the purposes of Contractor providing services to CDSS or otherwise to meet Contractor's obligations under the Agreement. For CDSS CSP, Contractor must provide CDSS Program Manager and CDSS Information Security Office with a list of Contractor authorized service providers and ensure they are bound by obligations sufficient to protect CDSS CSP in accordance with this 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. The 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. The Contractor and its employees, agents, or subcontractors 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 the 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. The Contractor shall retain each workforce member's background check documentation for a period of three (3) years following Agreement termination.

m. **Confidentiality Safeguards.** The 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 the 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. CDSS CSP information is not open to the public 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 wiped using the Gutmann or US Department of Defense (DoD) 5220.22-M (7 Pass) standard, or by degaussing. Media may also be physically destroyed in accordance with NIST Special Publication 800-88. Other methods require prior written permission of the CDSS Information Security Office.

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.

2. **Warning Banners.** All systems containing CDSS CSP must display a warning banner 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 the 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 the 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 the Contractor confirms the recipient fax number before sending, takes precautions to ensure that the fax was appropriately received, maintains procedures to notify recipients if the 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

a. **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 1798.29(e), California Civil Code 1798.82(f), and State Administrative Manual (SAM) Section 5340, Incident Management.

b. **Discovery and Notification of Information Security Incidents and/or Breaches**. The Contractor shall notify the CDSS Program Contract Manager and the CDSS Information Security and Privacy Officer within one (1) business day by telephone call and email upon the discovery of the Information Security Incident and/or Breach affecting the security of CDSS CSP if the CDSS CSP was, or is reasonably believed to have been, acquired by an unauthorized person, or there is an intrusion, potential loss, actual loss, or unauthorized use or disclosure of the CDSS CSP is in violation of this Agreement, this provision, or applicable law. The Contractor shall take:

   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.

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 one (1) business day 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**. The Contractor shall promptly investigate Information Security Incidents and/or Breaches. 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 the Contractor shall cooperate fully in such investigations.

e. **Updates on Investigation**. The Contractor shall provide regular (at least once a week) email updates on the progress of the Information Security Incident and/or Breach investigation to the CDSS Program Contract Manager and the CDSS Information Security and Privacy Officer until they are no longer needed, as mutually agreed upon between the Contractor and the CDSS Information Security and Privacy Officer.

f. **Written Report**. The 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. To the extent Contractor has such information, the report shall include but not be limited to the following:

   i. Contractor point of contact information;

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

   iii. 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. Full, detailed corrective action plan, including information on measures that were taken to halt and/or contain the Information Security Incident and/or Breach.

g. **Cost of Investigation and Remediation**. Per SAM Section 5305.8, the Contractor shall be responsible for all costs incurred by CDSS due to Information Security Incidents and/or Breaches resulting from the 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 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, the Contractor shall initiate contact as indicated herein. CDSS reserves the right to make changes to the contact information below by giving written notice to the 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, Contractor's facilities, systems and procedures 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 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 2017 10

Information resources maintained by the California Department of Social Services (CDSS) and provided to Contractor may be confidential, sensitive, and/or personal. Confidential, Sensitive, and/or Personal (CSP) information is not open to the public 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 is 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: _____

Information Security Officer (or authorized official responsible for business' information security program)

Name (Printed): _____

Title: _____

Business Name: _____

Email Address: _____

Phone: _____

Signature: _____

Date Signed: _____