MEMORANDUM OF UNDERSTANDING BETWEEN THE CALIFORNIA DEPARTMENT OF SOCIAL SERVICES AND COUNTY OF FRESNO

A. Purpose

This Memorandum of Understanding ("MOU") is entered into by the California Department of Social Services (hereinafter referred to as "CDSS") and County of Fresno (hereinafter referred to as "County") for the purpose of establishing the terms, conditions, and limitations for the exchange of confidential information contained in various datasets. For the purposes of this MOU, CDSS and County may be referred to individually as the "Party" or collectively as the "Parties".

This MOU authorizes County to receive data from the CDSS in order to conduct the program evaluations described herein.

B. Background and Authority

The Legal Authority for this Agreement by which the Employment Development Department (EDD) provides confidential wage and unemployment insurance claim information to the California Department of Social Services (CDSS) is pursuant to Section 1095(ai) of the California Unemployment Insurance Code (UIC), which enables federal, state, or local government departments or agencies, or their contracted agencies, subject to federal law, including the confidentiality, disclosure, and other requirements set forth in Part 603 of Title 20 of the Code of Federal Regulations, to evaluate, research, or forecast the effectiveness of public social services programs administered pursuant to Division 9 (commencing with Section 10000) of the Welfare and Institutions Code, or Part A of Subchapter IV of Chapter 7 of the federal Social Security Act (42 U.S.C. Sec. 601 et seq.), when the evaluation, research, or forecast is directly connected with, and limited to, the administration of the public social services programs.

County is to be provided access to EDD quarterly base wage files ("EDD Confidential Data") for the sole purpose of conducting program evaluations. County shall use the EDD Confidential Data to understand labor market participation of its employment services clients (e.g., California Work Opportunity and Responsibility to Kids (CalWORKs), CalFresh Employment & Training, and County General Assistance program clients in and County of Fresno Department of Social Services).

C. Scope of Data Sharing

It is necessary for County to measure the effectiveness of welfare-to-work and employment services efforts of residents within its geographic area in order to provide valuable input into subsequent programmatic design and resource allocation decisions. Additionally, these analyses are a useful tool in developing caseload forecasts and adapting employment services programs in response to labor market trends.

County data does not currently include any information on employment or earnings of its program recipients, and the EDD Confidential Data are the only accessible source for tracking the earned income of clients after receiving employment services. Additionally, several files produced by the EDD are the only accessible data source for tracking the employment and earnings of welfare program recipients after leaving public assistance as well as unemployment and disability payments. Matching client data with the EDD Confidential Data provides County with robust employment and earnings data that can be tracked over time for specific groups of program clients.

County may use the following data sets acquired from CDSS:

1. **EDD Base Wage File**: Quarterly wage earnings for the most recent six (6) quarters available of all persons in the relevant county, 16 years or older and who received at least one month of public assistance in that county. The data extract includes quarter date; social security number; employer account number (EAN); and quarterly earnings. The base wage file shall enable Counties to track the employment records and earnings of current and former welfare recipients. Historical wage data up to five (5) years prior is also available upon special request for selected clients but would require a separate agreement.

2. **Employer Data**: This file is a subset of the Quarterly Census of Employment and Wages created by the Bureau of Labor Statistics. It contains California employer data, such as employer identification number (EIN), North American Industry Classification System (NAICS) industry classification code, employer trade name, street address, Federal Information Processing Standards (FIPS) county code, and total quarterly wages paid. Employer data is available upon special request.

3. **Unemployment/Disability (UI/DI) Files**: UI/DI files track the unemployment and disability benefits of welfare recipients. Data includes time of payment, payment amount, social security number, and client name. This data is available upon special request for selected clients, subject to the CDSS cost review and available funds.

County will use EDD Confidential Data to enable, with respect to the content and function of the reports that County will create, the accurate measurement of the following program outcomes:

1. The number and proportion of clients with earned income;
2. The total earnings of clients and their wage progression over time;
3. The continuity of employment over time; and
4. How outcomes differ across various socioeconomic/demographic characteristics and specific employment services programs.

D. County Responsibilities

1. County shall provide a file to CDSS containing unduplicated client social security numbers and birth data, preferably in SAS or Excel/CSV format, in order to link administrative county data to the EDD Confidential Data.

2. County shall instruct all employees, agents, or volunteers with access to the information provided through this MOU as to the following:

   a. The confidential nature of the EDD Confidential Data;
   b. The requirements of Division 19 of the CDSS Manual of Policies and Procedures for the protection of confidential information provided by the CDSS or held by the County in its administration of social services;
   c. The need to adhere to the security and confidentiality provisions outlined in Exhibit E – Protection of Confidentiality Provisions; and
   d. Exhibit C, the EDD/CDSS Agreement.

3. Use of EDD Confidential Data shall be directly related to only the purposes discussed in this MOU.

4. **Under no circumstances shall individual client data be disclosed or used to contact individual persons. All data shall be reported in aggregate to protect client privacy. All reports shall comply with the California Health and Human Services (CHHS) Agency De-Identification Guidelines.**

5. County shall request a Project Request Review form from the CDSS Contract Contact prior to each proposed re-disclosure of the EDD Confidential Data. Once completed, County shall return the completed Project Request Review form to the CDSS Contract Contact, who will submit it to the CDSS Data Use Contact for approval. If approved, the CDSS Data Use Contact will then submit the Project Request Review to EDD for final approval. Project Request Reviews should be submitted at least ninety (90) calendar days prior to the date that County intends to begin use of EDD Confidential Data. Project Request Review approvals are only valid for the specified re-disclosure and parameters submitted and reviewed in the applicable Project Request Review form.

6. County shall include a disclaimer that credits any analyses, interpretations, or conclusions reached to the authors and not to the CDSS. The disclaimer shall be in substantially the following form, unless the Parties agree otherwise in writing:

"The research reported herein was performed with the permission of the California Department of Social Services. The opinions and conclusions expressed herein are solely those of the author(s) and should not be considered as representing the policy of any agency of the California State Government."

7. County shall provide CDSS with a pre-publication draft of any reports ninety (90) days before publication. A "report" is any document, email, or website that includes outcomes, results, or findings using EDD Confidential Data that is made available to the public. EDD requires all publications using EDD Confidential Data to be reviewed and approved by their Information Security Office prior to publication. The CDSS shall respond within ninety (90) calendar days from receipt of the pre-publication draft, thereby allowing both organizations the opportunity for resolution of any possible issues. The CDSS shall facilitate the approval process between County and EDD. Should the CDSS disagree with any part of the report, a disclaimer stating the CDSS's disagreement shall be included in the final published report.

8. County shall allow the CDSS to conduct random on-site inspections, as needed, to ensure compliance with the terms of the MOU.

E. CDSS Responsibilities

1. The CDSS shall provide the EDD Confidential Data for the purposes specified in this MOU.

2. The CDSS shall facilitate the linkage of client records provided by County to EDD base wage administrative files for this MOU. The process shall require CDSS to transmit client records to EDD; EDD performs the actual linkage (matching) and shall make the matched records available to CDSS for access and subsequent distribution to County. This linkage requires a valid social security number and date of birth for each client.

F. AUTHORIZED REPRESENTATIVE:

The authorized representatives during the term of this MOU shall be:

CDSS
Data Contact:
Cate Bird, Research Data Specialist II
Fiscal Forecasting Branch
744 P Street, MS 08-14-90
Sacramento, CA 95814
Cate.Bird@dss.ca.gov
Phone: (916) 651-1092

Data Use Contact:
Data Access Unit, Data Stewardship & Integrity Bureau
Enterprise Data Management Branch
744 P Street, MS 8-5-26
Sacramento, CA 95814
DataAccessUnit@dss.ca.gov

Program Contract Contact:
Sadie Webb
CalWORKs Engagement Bureau
744 P Street, MS 8-8-33
Sacramento, CA 95814
Sadie.Webb@dss.ca.gov

County of Fresno
The Contractor shall designate a person to be responsible for the security and confidentiality of the data. The Contractor shall **immediately** notify CDSS in writing of a designee change.

Security Contact:
Toribio Garcia, Staff Analyst
205 West Pontiac Way, Building 2
Clovis, CA 93612
Phone: (559) 600-2339
togarcia@fresnocountyca.gov

Program Contact:
Fasil Tilahun, Social Services Program Supervisor
3500 Never Forget Lane, Building 1
Clovis, CA 93612
Phone: (559) 600-5391
ftilahun@fresnocountyca.gov

Contract Contact:
Christina Flores, Senior Staff Analyst
205 West Pontiac Way, Building 2
Clovis, CA 93612
Phone: (559) 600-3061
cvflores@fresnocountyca.gov

Changes to this section do not require an amendment to this Agreement. The parties may change any of the above contacts by providing written notice to the other party within five (5) business days of the change.

G. TERM

This MOU shall be effective upon the signature of both the CDSS and County until terminated with 30 calendar days' written notice by either party.

H. GENERAL PROVISIONS

1. **Precedence.** The terms of the EDD and the CDSS agreement that provides authority and disclosure of data to this MOU shall take precedence over any conflicting terms or conditions set forth in any other part of the Agreement between County and the CDSS. Changes to the EDD and the CDSS Agreement may occur from time to time. Any such change to the EDD and CDSS Agreement will be provided to County in writing.

2. **Amendment**. This MOU may be amended by written mutual consent of the Parties.

3. **Termination**.

   a. Termination without cause: This MOU may be terminated by either party without cause upon 30 calendar 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 B. Background and Legal Authority, above, as being related to or necessary for the performance of this MOU, terminates or expires, this MOU shall 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) calendar days written notice. If this MOU is terminated for any reason, County shall immediately provide to the CDSS a copy of any completed and uncompleted report, writing, or other work product resulting from this MOU.

4. **Disputes.** If a dispute arises in connection with this MOU involving the interpretation, implementation, or conflicts of laws, policies and regulations, County and the CDSS will meet and attempt to resolve the problem in a manner that is allowable under the laws of the State of California.

5. **Survival**. All provisions of this MOU relating to privacy, confidentiality and information security, including Confidentiality and Security Requirements, shall survive the termination or expiration of this MOU.

I. AUTHORIZED REPRESENTATIVES

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

AGREED:

CALIFORNIA DEPARTMENT OF SOCIAL SERVICES

By: _____
Sharon Hoshiyama
Section Chief
Grants, MOU, Child Care Direct Services

Date: _____

COUNTY OF FRESNO

By: _____
Ernest Buddy Mendes
Chairman of the Board of Supervisors
of the County of Fresno

Date: _____

Attest:
Bernice E. Seidel
Clerk of the Board of Supervisors
County of Fresno, State of California

By: _____
Deputy

EMPLOYMENT DEVELOPMENT DEPARTMENT

CONFIDENTIALITY AGREEMENT

Information resources maintained by the State of California Employment Development Department (EDD) and provided to your agency may be confidential or sensitive. Confidential and sensitive information are not open to the public and require special precautions to protect it from wrongful access, use, disclosure, modification, and destruction. The EDD strictly enforces information security. If you violate these provisions, you may be subject to administrative, civil, and/or criminal action.

_____ an employee of _____
PRINT YOUR NAME — PRINT YOUR EMPLOYER'S NAME

hereby acknowledge that the confidential and/or sensitive records of the Employment Development Department are subject to strict confidentiality requirements imposed by state and federal law include the California Unemployment Insurance Code (UIC) §§1094 and 2111, the California Civil Code (CC) §1798 et seq., the California Penal Code (PC) §502, Title 5, USC §552a, Code of Federal Regulations, Title 20 part 603, and Title 18 USC §1905.

_____ INITIAL acknowledge that my supervisor and/or the Contract's Confidentiality and Data Security Monitor reviewed with me the confidentiality and security requirements, policies, and administrative processes of my organization and of the EDD.

_____ INITIAL acknowledge responsibility for knowing the classification of the EDD information I work with and agree to refer questions about the classification of the EDD information (public, sensitive, confidential) to the person the Contract assigns responsibility for the security and confidentiality of the EDD's data.

_____ INITIAL acknowledge responsibility for knowing the privacy, confidentiality, and data security laws that apply to the EDD information I have been granted access to by my employer, including UIC §§1094 and 2111, California Government Code § 15619, CC § 1798.53, and PC § 502.

_____ INITIAL acknowledge that wrongful access, use, modification, or disclosure of confidential information may be punishable as a crime and/or result in disciplinary and/or civil action taken against me—including but not limited to: reprimand, suspension without pay, salary reduction, demotion, or dismissal—and/or fines and penalties resulting from criminal prosecution or civil lawsuits, and/or termination of contract.

_____ INITIAL acknowledge that wrongful access, inspection, use, or disclosure of confidential information for personal gain, curiosity, or any non-business related reason is a crime under state and federal laws.

_____ INITIAL acknowledge that wrongful access, use, modification, or disclosure of confidential information is grounds for immediate termination of my organization's Contract with the EDD.

_____ INITIAL agree to protect the following types of the EDD confidential and sensitive information:

- Wage Information
- Employer Information
- Claimant Information
- Tax Payer Information
- Applicant Information
- Proprietary Information
- Operational Information (manuals, guidelines, procedures)

_____ INITIAL hereby agree to protect the EDD's information on either paper or electronic form by:

- Accessing or using the EDD supplied information only as specified in the Contract for the performance of the specific work I am assigned.
- Never accessing information for curiosity or personal reasons.
- Never showing or discussing sensitive or confidential information to or with anyone who does not have the need to know.
- Placing sensitive or confidential information only in approved locations.
- Never removing sensitive or confidential information from the work site without authorization.
- Following encryption requirements for all personal, sensitive, or confidential information in any portable device or media.

"I certify that I have read and initialed the confidentiality statements printed above and will abide by them."

_____
Print Full Name (last, first, MI)

_____
Signature

_____
Print Name of Requesting Agency

_____
Date Signed

Check the appropriate box:

☐ Employee ☐ Student

☐ Subcontractor ☐ Volunteer

☐ Other _____
Explain

The California Department of Social Services
Confidentiality and Information Security Requirements

State Agency/Entity - v 2022 01

This Confidentiality and Information Security Requirements Exhibit (hereinafter referred to as "this Exhibit") sets forth the information security and privacy requirements the State Agency/Entity as defined by the State Administrative Manual (SAM) Section 4819.2 (hereinafter referred to as "State Entity") is obligated to follow with respect to all confidential and sensitive information (as defined herein) disclosed to or collected by State Entity, pursuant to State Entity's Agreement (the "Agreement") with the California Department of Social Services (hereinafter "CDSS") in which this Exhibit is incorporated. The CDSS and State Entity 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 State Entity and CDSS.

II. Confidentiality of Information.

A. DEFINITIONS.

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

1. "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 7920.000 et seq.) or has restrictions on disclosure in accordance with other applicable state or federal laws.
2. "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 of which the disclosure would jeopardize the integrity of the CDSS (i.e., CDSS' fiscal resources and operations).
3. "Personal Information" is information in any medium (paper, electronic, or verbal) that alone, or in combination with other information, is linked or linkable to a specific individual in a manner that would allow a reasonable person in the community to be able to identify that individual with reasonable certainty. Personal Information includes, but is not limited to, information that identifies an individual (e.g., name, social security number,

driver's license number, home/mailing address, telephone number, financial matters with security codes, medical insurance policy number, Protected Health Information [PHI], etc.), personal characteristics that describe an individual (e.g., age, gender, race, ethnicity, language spoken, location of residence (including county), education status, financial status, physical description, sexual orientation, gender identity, medical history, employment history), and unique biometric data generated from measurements or technical analysis of human body characteristics (such as a fingerprint, retina, or iris image) used to authenticate a specific individual, but not a physical or digital photograph, unless used or stored for facial recognition purposes.

4. "Breach" is:
- **a.** the unauthorized acquisition, access, use, or disclosure of CDSS CSP in a manner which compromises the security, confidentiality or integrity of the information; or
- **b.** the same as the definition of "breach of the security of the system" set forth in California Civil Code section 1798.29(f).

5. "Information Security Incident" is:
- **a.** 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 State Entity and CDSS, including this Exhibit.

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

C. State Entity 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 7920.000 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

1. is or becomes generally known or available to the public other than because of a breach by State Entity of these confidentiality provisions;
2. already known to State Entity before receipt from CDSS without an obligation of confidentiality owed to CDSS;
3. provided to State Entity from a third party except where State Entity knows, or reasonably should know, that the disclosure constitutes a breach of confidentiality or a wrongful or tortious act; or
4. independently developed by State Entity without reference to the CDSS CSP.

III. State Entity Responsibilities.

A. Training.

State Entity shall instruct all employees, agents, and subcontractors with access to the CDSS CSP regarding:

1. The confidential nature of the information;
2. 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; and
3. CDSS procedures for reporting actual or suspected information security incidents in Paragraph IV - Information Security Incidents and/or Breaches.

B. Use Restrictions.

State Entity 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.

State Entity 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 State Entity receives a subpoena or other validly issued administrative or judicial notice requesting the disclosure of CDSS CSP, State Entity 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 State Entity's responsible unit for handling subpoenas and court orders.

E. Information Security Officer.

State Entity 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.

State Entity shall promptly transmit to the CDSS Program Contract Manager all requests for disclosure of any CDSS CSP, including Public Record Act (PRA) requests, (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.

State Entity 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 State Entity and CDSS, or upon a date mutually agreed upon by the Parties following expiration or termination, State Entity shall return or destroy the CDSS CSP. If return or destruction is not feasible, State Entity 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 State Entity 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, State Entity 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.

State Entity'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 State Entity returns or destroys the CDSS CSP or returns the CDSS CSP to CDSS; provided however, that on expiration or termination of the Agreement between State Entity and CDSS, State Entity 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 State Entity elects to destroy the CDSS CSP, State Entity 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. Personnel Management.

Before a member of State Entity's workforce may access CDSS CSP, State Entity agrees to implement personnel practices in compliance with SAM Section 5305.4 Personnel Management.

M. Confidentiality Acknowledgement.

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

N. Confidentiality Safeguards.

State Entity 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 and SAM Section 5300. Including at a minimum the following safeguards:

1. **Data Encryption.**

   All State Entity-owned or managed laptops, tablets, smart phones, and similar devices that process and/or store CDSS CSP must be encrypted per SAM Section 5350.1 and using a FIPS 140-2, until deprecated, certified algorithm which is 128 bit or higher, such as Advanced Encryption Standard (AES). It is also recommended to encrypt other computing devices such as workstations or desktops with full disk encryption.

2. **Data Transmission Encryption.**

   All data transmissions of CDSS CSP outside the secure internal network must be encrypted using a FIPS 140-2, until deprecated, certified algorithm and a Transport Layer Security (TLS) protocol version that has not deprecated to provide privacy and data integrity.

3. **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.

4. **Removable Media Devices.**

All electronic files that contain the CDSS CSP must be encrypted when stored on any removable media or portable device Encryption must be a FIPS 140-2, until deprecated, certified algorithm which is 128 bit or higher, such as AES.

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. **Antivirus Software.**

   All State Entity-owned or managed workstations, laptops, tablets, and similar devices that process and/or store CDSS CSP must install and actively use a comprehensive anti-virus software solution that complies with the State Office of Information Security (OIS) Information Management Manual (SIMM) 5355-A Endpoint Protection Standard.

7. **Patch Management.**

   To correct known security vulnerabilities, State Entity shall install security patches and updates in a timely manner on all State Entity-owned or managed workstations, laptops, tablets, smart phones, and similar devices that process and/or store CDSS CSP as appropriate based on State Entity's risk assessment of such patches and updates, the technical requirements of State Entity'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.

8. **Information Security Monitoring and Auditable Events.**

   For monitoring of its networks and other information assets, State Entity must comply with SAM Sections 5335 Information Security Monitoring and 5335.2 Auditable Events.

9. **Paper Document Controls.**

   State Entity shall safeguard CDSS CSP in accordance with SAM Section 5365.2 Media Protection.

10. **Confidential Destruction.**

    CDSS CSP must be disposed of through confidential means, such as crosscut shredding and/or pulverizing.

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

A. CDSS CSP Information Security Incidents and/or Breaches Response Responsibility.

State Entity shall be responsible for facilitating the Information Security Incident and/or Breach response process as described in California Civil Code 1798.29(e) and SAM Section 5340, Information Security Incident Management, including, but not limited to, taking:

1. 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
2. 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.

State Entity 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, considering the time necessary to allow State Entity 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. Investigation of Information Security Incidents and/or Breaches.

State Entity shall promptly investigate such 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 State Entity shall cooperate fully in such investigations. State Entity is not required to disclose their un-redacted confidential, proprietary, or privileged information. State Entity will keep CDSS fully informed of the results of any such investigation.

D. Updates on Investigation.

State Entity 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 State Entity and the CDSS Information Security and Privacy Officer. State Entity is not required to disclose their un-redacted confidential, proprietary, or privileged information.

E. Written Report.

State Entity 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. State Entity 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:

1. State Entity point of contact information;
2. 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;
3. 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;
4. A description of the unauthorized persons known or reasonably believed to have improperly used or disclosed CDSS CSP;
5. A description of where the CDSS CSP is believed to have been improperly transmitted, sent, or utilized;
6. A description of the probable causes of the improper use or disclosure;
7. Whether Civil Code sections 1798.29 or 1798.82 or any other federal or state laws requiring individual notifications of breaches are triggered; and
8. A full, detailed corrective action plan, including information on measures that were taken to halt and/or contain the Incident and/or Breach of CDSS CSP.

F. Cost of Investigation and Remediation.

Per SAM Section 5305.8, State Entity 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 State Entity'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. However, in accordance with California Civil Code §1798.29 any agency that owns or licenses computerized data shall do the notification.

V. Contact Information.

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

CDSS Program Contract Manager

See the Scope or Statement of Work exhibit for Program Project Representative information.

CDSS Information Security & Privacy Officer

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

VI. Plan of Action and Milestones (POAM).

The parties acknowledge that State Entity may have identified information security weaknesses or deficiencies where State Entity is not currently in full compliance with SAM and/or other applicable standards and/or requirements and, correspondingly, related provisions within this Exhibit. To the extent that those weaknesses or deficiencies have been identified and addressed by State Entity through the development of a POAM, the development of the POAM and the progress towards remediation of weaknesses or deficiencies on the POAM shall be deemed to be compliance with the terms of this Exhibit.

VII. Audits and Inspections.

CDSS may inspect and/or monitor the Contractor's system(s) or environment(s) if either contains, or is reasonably believed to contain, CDSS CSP in order to ensure compliance with physical or logical 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 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. CDSS Confidentiality and Security Compliance Statement

CALIFORNIA DEPARTMENT of SOCIAL SERVICES
CONFIDENTIALITY AND SECURITY COMPLIANCE STATEMENT v 2022 01

Information resources maintained by CDSS and provided to your entity 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 § 7920.000 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. State Entity 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 Agreement.

CDSS Representative:

Name (Printed):	Joseph Sapp
Title:	Staff Services Manager II
Business Name:	CDSS
Email Address:	Joseph.Sapp@dss.ca.gov
Phone:	(916) 858-9356
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:	