

Memorandum of Understanding

This Memorandum of Understanding (hereinafter referred to as "MOU") is between the California Department of Child Support Services (hereinafter referred to as "CDCSS"), 11120 International Drive, Rancho Cordova, CA 95710, and El Dorado County Department of Human Services, 3057 Briw Ridge Road, Suite A, Placerville, CA 95667, (hereinafter referred to as "Requestor") for the mutual administrative benefit of both parties. CDCSS shall provide to Requestor on-line access service to the Child Support Enforcement System (hereinafter referred to as "CSE") as specified herein for the purpose of supporting the Child and Spousal Support Enforcement Program pursuant to California Family Code Section 17212. The following terms and conditions apply to this MOU.

Contract Formation

1. This MOU is subject to any restrictions, limitations, or conditions enacted by the United States and the California State legislatures which may affect the provisions or terms herein in any manner.
2. This MOU, including any documents incorporated herein by express reference, is intended to be a complete integration and there are no prior or contemporaneous different or additional agreements pertaining to the subject matter of this MOU.
3. This MOU may only be modified in writing, signed by both parties.
4. This MOU is effective November 4, 2011 and shall be in effect for 36 months thereafter.
5. This MOU is subject to immediate termination by either party with cause.
6. Either party may terminate this MOU without cause upon thirty (30) days prior written notice of such termination. Notice is effective five (5) days from the date sent by facsimile (FAX) transmission or five (5) days from the date of mailing. Termination initiated by Requestor must be directed to the CDCSS contact described herein.
7. The MOU contacts and their respective contact information for this MOU are:

Lawrence Troxler California Department of Child Support Services Information Security Information Office P. O. Box 419064 Rancho Cordova, CA 95741-9064 Phone: 916-464-5774 FAX: 916-464-5772	Debbie Stack El Dorado County Department of Human Services 3057 Briw Ridge Road, Suite A Placerville, CA, 95667 Phone: 530-642-7325 FAX : 530-626-9060
---	---

Scope of CDCSS Services

8. CDCSS shall provide to Requestor the specified number of Users with CSE online access as follows.

Total Number of Users	5	List Profile for each User
Purpose of Requestor Access:		
Inquiries are necessary to ensure CDCSS absent parent(s) have made timely child support payments that are credited towards specific CalWORKS clients(s) for eligibility purposes in order to ensure compliance with time clock issues.		

- 9. CDCSS shall provide the Requestor online access to CSE Monday through Friday from 6 a.m. to 6 p.m.
- 10. CDCSS shall provide Requestor's online access to CSE via the Office of Technology Services wide area network.

General Obligations of Requestor

- 11. For the purposes of determining compliance with the terms of this MOU, Requestor shall allow audits or inspections by individuals authorized by CDCSS at Requestor's premises during regular business hours, upon three (3) business day's prior notice. CDCSS retains the right to examine records, security statements, computer data journals (system-generated), system storage media, network components, and access terminals applicable to this MOU to determine compliance.
- 12. Requestor shall implement and maintain the security of its system and components used for retrieval, transmittal, storage and services used to access CSE as described in this MOU.
- 13. Requestor acknowledges all information in CSE is confidential and must not be shared with unauthorized persons. Criminal and Civil Penalties may apply.
- 14. Requestor acknowledges that anyone who accesses CSE expressly consents to monitoring.
- 15. Requestor shall be responsible for the cost and maintenance of all communication connections between Requestor and Office of Technology Services.
- 16. Requestor shall, on an annual basis upon request of the DCSS information Security Officer (ISO), provide the name, work address, phone number, and e-mail address of all CSE users in an Excel format.

Security Provisions

- 17. Requestor shall implement the following administrative safeguards. Requestor shall:
 - a. Assign security and confidentiality responsibilities related to this MOU to its ISO and one additional contact listed below. Requestor shall notify CDCSS in writing as soon as practical of any designee changes.

Name and Title	Contact Information (Address, Phone & E-Mail)
Dianne Faiferek Staff Services Analyst II	3057 Briw Ridge Road, Suite A Placerville, CA 95667 530-642-7179 Dianne.Faiferek@edcgov.us
Joan Lopes Eligibility System Specialist	3057 Briw Ridge Road, Suite A Placerville, CA 95667 530- 573-4310 Joan.Lopes@edcgov.us

- b. Implement policies and procedures to ensure that information obtained from CSE is used solely as provided for in this MOU and applicable laws, including, but not limited to, Family Code, section 17212.
- c. Make information available to its authorized personnel on a "need-to-know" basis and only for the purposes authorized under this MOU. "Need -to-know" refers to those authorized persons who need information to perform their official duties in connection with the purpose described in this MOU.
- d. Notify CDCSS Information Security Office (ISO) of any information security breach involving information obtained from CSE as soon as practical, but no later than one (1)

hour after an event is detected as described in the Information Security Manual (ISM) at <http://www.childsup.ca.gov/Portals/0/home/docs/InfoSecurityManual.pdf>. Requestor shall cooperate with CDCSS ISO in any investigation(s) of information security incidents. The notification must describe the incident in detail and provide contact information if different from the Information Security Officer described herein. In the event of a security breach contact the ISO using the information below:

Information Security Office
Info.security@dcss.ca.gov
(916) 464-5045

- e. Requestor shall maintain a record of all authorized users and authorization level of access granted to CSE information based on job function. The record must include the name, work address, telephone number, and e-mail address. A copy of this record must be sent to the ISO within five business days when an authorized user is added or deleted. This can be accomplished by US Mail, FAX or scanned.
18. Requestor shall implement the following usage, duplication, and redisclosure safeguards. Requestor shall:
- a. Use information only for purposes specifically authorized under the MOU and applicable federal and State laws. including, but not limited to: Title 26 United States Code sections 7213(a), 7213A, and 7431; California Penal Code section 502; California Family Code section 17212; California Unemployment Insurance Code sections 1094, 2111, and 2122; California Revenue and Taxation Code sections 7056, 7056.5, 19542, and 19542.1; and California Civil Code section, et seq. 1798.
 - b. Protect CSE information against unauthorized access, at all times.
 - c. Reproduce information in any form obtained under this MOU solely for purposes described herein.
 - d. Refrain from publishing or selling information obtained under this MOU.
 - e. Transmit information obtained under this MOU solely for purposes described herein in a secure manner as described in the ISM, Section 2109.
19. Requestor shall implement the following physical safeguards for CSE information. Requestor shall:
- a. Secure and maintain any computer systems, hardware, software, applications, and data that shall be used in the performance of this MOU. This includes ensuring that all security patches, upgrades, and anti-virus updates are applied as appropriate to secure all information assets and data that may be used, transmitted, or stored on such systems in the performance of this MOU.
 - b. Safeguard equipment when used in public areas to access and view CSE information (e.g. during legal proceedings).
 - c. Restrict removal of CSE confidential information from Requestor's work location.
 - d. Store CSE information in a place physically secure from access by unauthorized persons.
20. Requestor shall implement the following management safeguards for CSE information. Requestor shall:
- a. Provide annual security awareness training to each User authorized to online access to CSE information pursuant to this MOU or who shall be provided access to downloaded CSE information on a need-to-know basis.
 - b. Annually, obtain signed confidentiality statements provided by CDCSS, from each User pursuant to this MOU.

- c. Maintain signed confidentiality statements in an easily retrievable format and make statements available to CDCSS upon request.
21. All changes to systems, storage media, and network components used for CSE online access or services must be consistent and compatible with CSE technical configuration requirements. To ensure compatibility and compliance, one of the local ISO, named in #19 of this document, must approve in writing all configurations prior to implementation. DCSS shall monitor compliance with this requirement. Refer to the ISM, found at this link <http://www.childsup.ca.gov/Portals/0/home/docs/InfoSecurityManual.pdf>.
22. Requestor shall ensure that an access control program shall consist of at a minimum, unique individual User Identifier and user-selected passwords for each person is utilized on every system capable of online CSE access. At a minimum, verification of manually keyed unique User Identifier and user-selected passwords shall be required for initiation of access.
23. Requestor shall ensure video terminals, printers, hard copy printouts or any other forms of CSE records are placed so that they may not be viewed by the public or other unauthorized persons. CSE information shall be destroyed when its business use has ended in a confidential manner such as incineration, mulching, pulping, disintegration, or shredding. Refer to DCSS ISM, 2110, Media Protection and Sanitation.
24. Requestor shall ensure terminals shall not be left unattended while in active logon access session to CSE information unless secured by functioning locking device which prevents entry, viewing or receipt of information or secured in a locked room which is not accessible to unauthorized personnel. All devices, which contain unique identification codes used by Requestor for verification of authorized access to CSE information, shall be secured against tampering.

Performance

25. The CSE contains Internal Revenue Service (IRS) data. In performance of this contract the Requestor agrees to comply with and assume responsibility for compliance by his or her employees with the following requirements:
 - a. All work shall be performed under the supervision of the Requestor or the Requestor's responsible employees.
 - b. Any return or return information made available in any format shall be used only for the purpose of carrying out the provisions of this contract. Information contained in such material shall be treated as confidential and shall not be divulged or made known in any manner to any person except as may be necessary in the performance of this contract. Disclosure to anyone other than an officer or employee of the Requestor shall be prohibited.
 - c. All returns and return information shall be accounted for upon receipt and properly stored before, during, and after processing. In addition, all related output shall be given the same level of protection as required for the source material.
 - d. The Requestor certifies that the data processed during the performance of this contract shall be completely purged from all data storage components of his or her computer facility, and no output shall be retained by the Requestor at the time the work is completed. If immediate purging of all data storage components is not possible, the Requestor certifies that any IRS data remaining in any storage component shall be safeguarded to prevent unauthorized disclosures.
 - e. Any spoilage or any intermediate hard copy printout that may result during the processing of IRS data shall be given to the agency or his or her designee. When this

is not possible, the Requestor shall be responsible for the destruction of the spoilage or any intermediate hard copy printout, and shall provide the agency or his or her designee with a statement containing the date of destruction, description of material destroyed, and the method used.

- f. All computer systems receiving, processing, storing, or transmitting Federal tax information must meet the requirements defined in IRS Publication 1075. To meet functional and assurance requirements, the security features of the environment must provide for the managerial, operational, and technical controls. All security features must be available and activated to protect against unauthorized use of and access to Federal tax information.
- g. No work involving Federal tax information furnished under this contract shall be subcontracted without prior written approval of the IRS.
- h. The Requestor shall maintain a list of employees authorized access. Such list shall be provided to the agency and, upon request, to the IRS reviewing office.
- i. The agency shall have the right to void the contract if the Requestor fails to provide the safeguards described above.

Criminal/Civil Sanctions

26. The CSE contains Internal Revenue Service (IRS) data.

- a. Each officer or employee of any person to whom returns or return information is or may be disclosed shall be notified in writing by such person that returns or return information disclosed to such officer or employee can be used only for a purpose and to the extent authorized herein, and that further disclosure of any such returns or return information for a purpose or to an extent unauthorized herein constitutes a felony punishable upon conviction by a fine of as much as \$5,000 or imprisonment for as long as five years, or both, together with the costs of prosecution. Such person shall also notify each such officer and employee that any such unauthorized future disclosure of returns or return information may also result in an award of civil damages against the officer or employee in an amount not less than \$1,000 with respect to each instance of unauthorized disclosure. These penalties are prescribed by IRC Sections 7213 and 7431 and set forth at 26 CFR 301.6103(n)-1.
- b. Each officer or employee of any person to who returns or return information is or may be disclosed shall be notified in writing by such person that any return or return information made available in any format shall be used only for the purpose of carrying out the provisions of this contract. Information contained in such material shall be treated as confidential and shall not be divulged or made known in any manner to any person except as may be necessary in the performance of this contract. Inspection by or disclosure to anyone without an official need to know constitutes a criminal misdemeanor punishable upon conviction by a fine of as much as \$1,000 or imprisonment for as long a 1 year, or both, together with the costs of prosecution. Such person shall also notify each such officer and employee that any such unauthorized inspection or disclosure of returns or return information may also result in an award of civil damages against the officer or employee [United States for Federal employees] in an amount equal to the sum of the greater \$1,000 for each act of unauthorized inspection or disclosure with respect to which such defendant is found liable or the sum of the actual damages sustained by the plaintiff as a result of such unauthorized inspection or disclosure plus in the case of a willful inspection or disclosure which is the

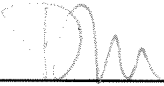
result of gross negligence, punitive damages, plus the costs of the action. The penalties are prescribed by IRC Sections 7213A and 7431.

- c. Additionally, it is incumbent upon the Requestor to inform its officers and employees of the penalties for improper disclosure imposed by the Privacy Act of 1974, 5 U.S.C. 552a. Specifically, 5 U.S.C. 552a(i)(1), which is made applicable to Requestors by 5 U.S.C. 552a(m)(1), provides that any officer or employee of a Requestor, who by virtue of his/her employment or official position, has possession of or access to agency records which contain individually identifiable information, the disclosure of which is prohibited by the Privacy Act or regulations established there under, and who knowing that disclosure of the specific material is so prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than \$5,000.


Inspection

- 27. The IRS and the Agency shall have the right to send its officers and employees into the offices and plants of the Requestor for inspection of the facilities and operations provided for the performance of any work under this contract. On the basis of such inspection, specific measures may be required in cases where the Requestor is found to be noncompliant with safeguards.
- 28. **Administrator:** The County Officer or employee with responsibility for administering this Agreement is Debbie Stack, Program Manager, Department of Human Services, or successor.

REQUESTING CONTRACT ADMINISTRATOR CONCURRENCE:

By:  Dated: 10/24/11
 Debbie Stack
 Program Manager
 Department of Human Services

REQUESTING DEPARTMENT HEAD CONCURRENCE:

By:  Dated: 10-25-2011
 Daniel Nielson, M.P.A.
 Director
 Department of Human Services

//

//

Execution of Signatories

I have read and understand the MOU and agree to abide by the terms and conditions herein.

**--- STATE OF CALIFORNIA ---
--- DEPARTMENT OF CHILD SUPPORT SERVICES ---**

By: _____ Dated: _____
Lawrence Troxler
Information Security Officer
Information Privacy Officer

Division: Information Security Office

--- COUNTY OF EL DORADO ---

By: _____ Dated: _____
Raymond J. Nutting, Chair
Board of Supervisors
"Requestor"

ATTEST:
Suzanne Allen de Sanchez
Clerk of the Board of Supervisors

By: _____ Dated: _____
Deputy Clerk