

**CALIFORNIA DEPARTMENT OF CHILD SUPPORT SERVICES**

P.O. Box 419064, Rancho Cordova, CA 95741-9064



March 22, 2012

LCSA LETTER: 12-05

ALL IV-D DIRECTORS

SUBJECT: **MEDI-CAL ELIGIBILITY DETERMINATION  
SYSTEM AND INCOME ELIGIBILITY VERIFICATION  
SYSTEM ENHANCED SECURITY REQUIREMENTS**

<u>Reason for this Transmittal</u>
<input type="checkbox"/> State Law or Regulation Change
<input type="checkbox"/> Federal Law or Regulation Change
<input type="checkbox"/> Court Order or Settlement Change
<input type="checkbox"/> Clarification requested by One or More Counties
<input checked="" type="checkbox"/> Initiated by DCSS

The purpose of this letter is to inform the local child support agencies (LCSAs) of the enhanced security requirements for the LCSAs who access the Medi-Cal Eligibility Determination System (MEDS) and the Income Eligibility Verification System (IEVS).

The Department of Health Care Services (DHCS) and the Department of Child Support Services (DCSS) entered into an Interagency Agreement that requires DCSS to implement and maintain data privacy and Security Agreements (Agreement) with each LCSA representative who accesses MEDS or IEVS.

To assist with this new effort, the DCSS Information Security Office (ISO) has established a 'DCSS MEDS Security Coordinator'. The role of the 'Coordinator' is to manage the Agreement, to ensure each is completed in a timely manner, renewed after 36 months and provide security related direction to the LCSAs.

Upon receipt of this letter, and the related Agreement; each LCSA will make two copies of the Agreement, the LCSA Director will sign both documents and return one to DCSS ISO within 30 business days from date of this letter, to the following address:

California Department of Child Support Services  
Attn: Barbara Lamb  
Information Security Office  
P. O. Box 419064 – MS 440  
Rancho Cordova, CA 95741-9064

LCSA Letter: 12-05

March 22, 2012

Page 2

If you have any questions please contact Barbara Lamb at 916-464-5720, or via email at [Barbara.Lamb@dcss.ca.gov](mailto:Barbara.Lamb@dcss.ca.gov).

Sincerely,

/os/

JUDY RAMOS

Interim Information Security Officer

Attachment

Security Agreement

Department of Child Support Services  
Information Security Office  
Medi-Cal Data Privacy and Security Agreement  
Between the Department of Child Support Services and  
\_\_\_\_\_ Local Child Support Agency

---

**PREAMBLE**

The California Department of Child Support Services (DCSS) and the \_\_\_\_\_ County Local Child Support Agency (LCSA) enter into this Medi-Cal Data Privacy and Security Agreement (“Agreement”) in order to ensure the privacy and security of Medi-Cal Personally Identifiable Information (PII) contained in the Medi-Cal Eligibility Determination System (MEDS) and Income and Eligibility Verification System (IVES), collectively known as MEDS.

DCSS partners with the Department of Health Care Services (DHCS) to obtain electronic access to PII to support the child support program. Because the Social Security Administration (SSA) is the source of some information, all LCSAs that access SSA information must enter into this Agreement.

In this Agreement, PII shall have the following meaning:

- A. “Medi-Cal PII” is information directly obtained in the course of performing an administrative function on behalf of Medi-Cal, such as determining Medi-Cal eligibility or conducting In-Home Supportive Services (IHSS) operations, that can be used alone, or in conjunction with any other information, to identify a specific individual. PII includes any information that can be used to search for or identify individuals, or can be used to access their files, such as name, social security number, date of birth, driver’s license number or identification number. PII may be electronic or paper.

This Agreement covers the County of \_\_\_\_\_ LCSA workers who access Medi-Cal program data for the purpose of supporting the child support program. The LCSA will compare information with Child Support data for the purpose of obtaining critical information related to non-custodial parents. The Agreement is effective on the date executed by the DCSS Information Security Officer (ISO) and shall be in effect for 36 months thereafter.

## **AGREEMENTS**

**NOW THEREFORE**, DCSS and the LCSA mutually agree as follows:

### **I. PRIVACY AND CONFIDENTIALITY**

- A. LCSA workers covered by this Agreement (“LCSA Workers”) may access PII only to perform functions or activities directly related to the administration of the Child Support Program. No LCSA Worker shall duplicate, disseminate or disclose PII except as allowed in this Agreement.
- B. Access to PII shall be restricted to only LCSA Workers who need the PII to perform their official duties in connection with the administration of the Child Support Program.
- C. LCSA Workers, who access, disclose or use PII in a manner or for a purpose not authorized by this Agreement may be subject to civil and criminal sanctions contained to applicable federal and state statutes.
- D. Access may be terminated if unauthorized access is permitted.

### **II. EMPLOYEE TRAINING AND DISCIPLINE**

The LCSA agrees to advise and train LCSA Workers who have access to PII of the confidentiality of the information, the safeguards required to protect the information, and the civil and criminal sanctions for non-compliance contained in the applicable Federal and State laws. These laws are outlined in The DCSS Information Security Manual (ISM), Sections 2000, 2100, 2103, 2109, 3000, 5000 and 6000. The DCSS ISM can be found at the following location: <http://www.childsup.ca.gov/Portals/0/home/docs/InfoSecurityManual.pdf>.

For that purpose, the LCSA shall:

- A. Train and use reasonable measures to ensure compliance with the requirements of this Agreement by LCSA Workers who assist in the administration of the Child Support Program and view PII; and take corrective action against such LCSA Workers who intentionally violate any provisions of this Agreement, up to and including termination of employment. In complying with this requirement, the LCSA agrees to:
  - 1. Provide privacy and security awareness training to each new LCSA Worker within 30 days of employment and thereafter provide ongoing reminders of the privacy and security safeguards in this Agreement to all LCSA Workers who access PII.

2. Maintain records indicating each LCSAs name and the date on which the initial privacy and security awareness training was completed.
3. Retain training records for inspection for a period of three years after completion of training.

### **III. MANAGEMENT OVERSIGHT AND MONITORING**

The MEDS uses Resource Access Control Facility (RACF) software to record access. RACF logs the activity of all users including unsuccessful attempts to access the MEDS. Users should not assume any privacy when accessing the MEDS as all actions are electronically logged. LCSA Workers who access the MEDS shall agree to be monitored.

The LCSA agrees to:

- A. Establish and maintain ongoing Management oversight and quality assurance for monitoring workforce compliance with the privacy and security safeguards in this Agreement while accessing PII as described in the MEDS Security and Procedures Manual, (Exhibit A).
- B. Ensure that ongoing Management oversight includes periodic self assessments and randomly sampling work activity by LCSA Workers who assess PII. The DHCS shall provide the LCSAs with information on MEDS usage indicating any anomalies for investigation and follow-up.
- C. Ensure that these Management oversight and monitoring activities are performed by LCSA Workers whose job functions are separate from those who use PII as part of their routine duties.
- D. Upon request, work with The DCSS ISO to develop, enhance or maintain oversight activities. As well as, respond to questions and or concerns regarding MEDS access and security.

The LCSA MEDS Coordinator agrees to:

- A. On a quarterly basis, review records and ensure personnel who no longer require access are deleted from the MEDS.
- B. Develop and or maintain control and oversight processes to ensure only authorized users access the MEDS. Upon request, provide a copy of written procedures to The DCSS ISO and or The DHCS.

- C. Identify LCSA MEDS Coordinator (and at least one backup) and provide contact information to include the items listed below, to the DCSS MEDS Coordinator. Notify the DCSS MEDS Coordinator of any changes regarding these designations within five (5) business days.

LCSA MEDS Coordinator
County, Department of Child Support Services
LCSA MEDS Coordinator Name:
Address:
City, CA ZIP Code:
E-Mail Address:
Phone Number:

- D. Notify the DCSS ISO immediately or within one (1) hour of any suspicious activity or unauthorized access. Use the instructions outlined in “Section VIII, Notification and Investigation of Breaches”, in this document.

#### **IV. CONFIDENTIALITY STATEMENT**

The LCSA agrees to ensure that all LCSA Workers who access PII sign a confidentiality statement. The statement shall include at a minimum, General Use, Security and Privacy Safeguards, Unacceptable Use, and Enforcement Policies. The statement shall be signed by the LCSA Worker prior to access to PII. See Exhibit B.

#### **V. PHYSICAL SECURITY**

The LCSA shall ensure that PII is used and stored in an area that is physically safe from access by unauthorized persons during working hours and non-working hours. The LCSA agrees to safeguard PII from loss, theft, or inadvertent disclosure as described by the provisions of the DCSS ISM, Section 2108 or equivalent Information Security Policy.

#### **VI. COMPUTER SECURITY SAFEGUARDS**

The LCSA agrees to comply with the general computer security safeguards, system security controls, and audit controls in this section (General Computer Security Safeguards).

##### **General Computer Security Safeguards**

In order to comply with the following general computer security safeguards, the LCSA agrees to:

- A. Encrypt portable computer devices, such as laptops and notebook computers that assess PII, with a solution using a vendor product that is recognized as an industry leader in meeting the needs for the intended solution. One source of recommended solutions is specified by the California Strategic Sourced Initiative (CSSI) located at the following link: [www.pd.dgs.ca.gov/masters/EncryptionSoftware.html](http://www.pd.dgs.ca.gov/masters/EncryptionSoftware.html). The LCSA shall use an encryption solution that is full-disk unless otherwise approved by The DHCS.
- B. Encrypt workstations where PII is stored using a vendor product that is recognized as an industry leader in meeting the needs for the intended solution, such as products specified by the CSSI.
- C. Ensure that only the minimum necessary amount of PII is downloaded to a laptop or hard drive when absolutely necessary for current business purposes.
- D. Encrypt all electronic files that contain PII when the file is stored on any removable media type device (i.e. USB thumb drives, floppies, CD/DVD, etc.) using a vendor product that is recognized as an industry leader in meeting the needs for the intended solution, such as products specified by the CSSI.
- E. Ensure that all emails sent outside the LCSA e-mail environment that include PII are sent via an encrypted method using a vendor product that is recognized as an industry leader in meeting the needs for the intended solution, such as products specified by the CSSI.
- F. Ensure that all workstations, laptops and other systems that process and/or store PII have a commercial third-party anti-virus software solution and are updated when a new anti-virus definition/software release is available.
- G. Ensure that all workstations, laptops and other systems that process and/or store PII have current security patches applied and are up-to-date.
- H. Ensure that all PII is wiped from systems when the data is no longer legally required. The LCSA shall ensure that the wipe method conforms to Department of Defense standards for data destruction.
- I. Ensure that any remote access to PII is established over an encrypted session protocol using a vendor product that is recognized as an industry leader in meeting the needs for the intended solution, such as products specified by the CSSI. The LCSA shall ensure that all remote access is limited to the minimum necessary and the least privilege principles.

## **System Security Controls**

In order to comply with the following system security controls, the LCSA agrees to adhere to the Access Control Standards referenced in the DCSS ISM, Section 2100, or equivalent Information Security Policy. The LCSA agrees to:

- A. Ensure that all LCSA systems that access PII provide an automatic timeout after no more than 20 minutes of inactivity.
- B. Ensure that all LCSA systems containing PII display a warning banner stating that data is confidential, systems are logged, and system use is for business purposes only. Users shall be directed to log off the system if they do not agree with these requirements.
- C. Ensure that all LCSA systems containing PII log successes and failures of user authentication and authorizations granted. The system shall log all data changes and system accesses conducted by all users (including all levels of users, system administrators, developers, and auditors). The system shall have the capability to record data access for specified users when requested by authorized Management personnel. A log of all system changes shall be maintained and be available for review by authorized Management personnel.
- D. Ensure that all LCSA systems containing PII use role based access controls for all user authentication, enforcing the principle of least privilege.
- E. Ensure that all LCSA data transmissions over networks outside of the LCSAs control are encrypted end-to-end using a vendor product that is recognized as an industry leader in meeting the needs for the intended solution, such as products specified by the CSSI, when transmitting PII. The LCSA shall encrypt PII at the minimum of 128 bit AES or 3DES (Triple DES) if AES is unavailable.
- F. Ensure that all LCSA systems that are accessible via the Internet or store PII actively use either a comprehensive third-party real-time host based intrusion detection and prevention program or be protected at the perimeter by a network based IDS/IPS solution.

## **Audit Controls**

In order to comply with the following audit controls, the LCSA agrees to comply with the DCSS ISM, Section 2100, or equivalent Information Security Policy.

The LCSA agrees to:

- A. Ensure that all LCSA systems that view, process and/or store PII have at least an annual system security review. The LCSA review shall include administrative and technical vulnerability assessments.
- B. Ensure that all LCSA systems processing and/or storing PII have an automated audit trail, which includes the initiator of the request, along with a time and date stamp for each access. These logs shall be read-only and maintained for a period of at least three (3) years. There shall be a routine procedure in place to review system logs for unauthorized access. The LCSA shall investigate anomalies identified by interviewing LCSA Workers and witnesses and taking corrective action, including by disciplining LCSA Workers, when necessary.
- C. Maintain an automated audit trail record identifying either the individual LCSA Worker or the system process that initiated a request for information from the SSA for its systems, such as IEVS. Individual audit trail records shall contain the data needed to associate each query transaction to its initiator and relevant business purpose (that is, the client record for which SSA data was accessed) and each transaction shall be time and date stamped. Access to the audit file shall be restricted to authorized users with a need to know and the audit file data shall be unalterable (read only) and maintained for a minimum of three (3) years.
- D. Investigate anomalies in MEDS usage identified by The DHCS and report conclusions of such investigations and remediation to The DHCS and The DCSS ISO.
- E. Exercise Management control and oversight, in conjunction with The DHCS, of the function of authorizing individual user access to SSA data and MEDS and over the process of issuing and maintaining access control numbers and passwords.
- F. Ensure that all LCSA systems processing and/or storing PII have a documented change control procedure that ensures separation of duties and protects the confidentiality, integrity and availability of data.

## **VII. PAPER DOCUMENT CONTROLS**

In order to comply with the following paper document controls, the LCSA agrees to adhere to DCSS ISM, Sections 2110 and 2111, or equivalent Information Security Policy. The LCSA agrees to:

- A. Dispose of PII in paper form through confidential means, such as cross cut shredding and pulverizing.
- B. Not remove PII from the premises of the LCSA except for identified routine business purposes or with express written permission of The DHCS and The DCSS ISO.
- C. Not leave faxes containing PII unattended and keep fax machines in secure areas. The LCSA shall ensure that faxes contain a confidentiality statement notifying persons receiving faxes in error to destroy them. The LCSA Workers shall verify fax numbers with the intended recipient before sending.
- D. Use a secure, bonded courier with signature of receipt, when sending large volumes of PII. The LCSA shall ensure that disks and other transportable media sent through the mail are encrypted using a vendor product that is recognized as an industry leader in meeting the needs for the intended solution, such as products specified by the CSSI.

**VIII. NOTIFICATION AND INVESTIGATION OF BREACHES**

In the event of a breach the LCSA agrees to notify The DHCS and The DCSS ISO.

- A. Notify The DHCS immediately by telephone call or e-mail upon the discovery of a breach of security of PII in computerized form if the PII was, or is reasonably believed to have been acquired by an unauthorized person; or within 24 hours by telephone call or e-mail of discovery of any other suspected security incident, intrusion, loss or unauthorized use or disclosure of PII in violation of this Agreement or law. The LCSA shall submit the notification to The DHCS Privacy Officer and The DHCS ISO. If the incident occurs after business hours on a weekend or holiday and involves electronic PII, the LCSA shall notify The DHCS by calling The DHCS ITSD Help Desk.

DHCS Privacy Officer	DHCS Information Security Officer
Privacy Officer c/o Office of Legal Services Department of Health Care Services P.O. Box 997413, MS 0011 Sacramento, CA 95899-7413	Information Security Officer DHCS Information Security Office P.O. Box 997413, MS 6400 Sacramento, CA 95899-7413
Email: <a href="mailto:privacyofficer@dhcs.ca.gov">privacyofficer@dhcs.ca.gov</a>	Email: <a href="mailto:iso@dhcs.ca.gov">iso@dhcs.ca.gov</a>
Telephone: (916) 445-4646	Telephone: ITSD Help Desk (916) 440-7000 (800) 579-0874

- B. Notify The DCSS ISO no later than one (1) hour or as soon as practical. See DCSS ISM, Section 3100, or equivalent Information Security Policy.
  - 1. Complete and submit a Security Event Report (Attachment C) via email to The DCSS ISO within five working days of reporting the event.

<b>Report Security Breaches</b>
Email: <a href="mailto:info.security@dcss.ca.gov">info.security@dcss.ca.gov</a>
Phone: 916-464-5045

- 2. Take prompt corrective action to mitigate any risks or damages involved with the breach and to protect the PII.

DCSS shall: Investigate the event, make corrective actions and notify appropriate parties according to the Incident Reporting Requirements outlined in the DCSS ISM, Section 3100, or equivalent Information Security Policy.

## **IX. COMPLIANCE WITH SSA AGREEMENTS**

The LCSA agrees to comply with substantive privacy and security requirements in the Agreement between Social Security Administration (SSA) and DHCS, known as the 1137 Agreement, which is hereby incorporated into this Agreement. The specific sections of the 1137 Agreement which contain substantive privacy and security requirements which are to be complied with by LCSA are as follows: XI. Procedures for Security; XII. Safeguarding and Reporting Responsibilities for Personally Identifiable Information (PII); XIII. Procedures for Records Usage, Duplication, and Redisclosure Restrictions; and Attachment A.1, Information System Security Guidelines for Federal, State and Local Agencies Receiving Electronic Information from the SSA. If there is any conflict between privacy and security standard in these sections of the 1137 Agreement and a standard in this Agreement, the most stringent standard shall apply. The most stringent standard means, standards which provides the greatest protection to data.

## **X. COMPLIANCE BY LCSA**

The LCSA shall require that any agents, including subcontractors, which assist the LCSA in its authorized functions and to which the LCSA provides PII, agree to the same privacy and security safeguards as are contained in this Agreement; and to incorporate, when applicable, the relevant provisions of this Agreement into each subcontract or sub-award to such agents or subcontractors.

## **XI. ASSESSMENTS AND REVIEWS**

In order to enforce this Agreement and ensure compliance with its provisions, the LCSA agrees to allow The DHCS and The DCSS ISO to inspect the facilities, systems, books and records of the LCSA, with reasonable notice from The DCSS ISO, in order to perform assessments and reviews. Such inspections shall be scheduled at times that take into account the operational and staffing demands of the LCSA. The LCSA agrees to promptly remedy any violation of any provision of this Agreement and certify the same to The DCSS ISO in writing, or to enter into a written corrective action plan with The DCSS ISO containing deadlines for achieving compliance with specific provisions of this Agreement.

## **XII. DEADLINE FOR SUBSTANTIAL COMPLIANCE**

- A. The LCSA shall be in substantial compliance with this Agreement by no later than April 10, 2012.
- B. If, at any time, the LCSA is unable to meet the security and privacy requirements imposed in this Agreement in the manner specified therein due to a lack of funding; DCSS will work with the LCSA to develop a Corrective Action Plan which can be implemented within the resources provided by the DCSS for this purpose and which is intended to substantially meet those security and privacy requirements even if such requirements are met utilizing alternative or different methods than those specified in this Agreement.
- C. The DCSS ISO shall monitor Corrective Action Plans which LCSAs develop to remediate gaps in security compliance under this Agreement and reassess compliance.

## **XIII. ASSISTANCE IN LITIGATION OR ADMINISTRATIVE PROCEEDINGS**

In the event of litigation or administrative proceedings involving The DHCS based upon claimed violations by the LCSA of the privacy or security of PII, or Federal or State laws or agreements concerning privacy or security of PII, the LCSA shall make all reasonable effort to make itself and any subcontractors, agents, and LCSA Workers assisting in the administration of the Medi-Cal Program and using or disclosing PII available to The DHCS at no cost to The DHCS to testify as witnesses. The DHCS shall also make all reasonable efforts to make itself and any subcontractors, agents, and employees available to the LCSAs and The DCSS at no cost to the LCSAs and The DCSS to testify as witnesses, in the event of litigation or administrative proceedings involving the LCSA based upon claimed violations by The DHCS of the privacy or security of PII, or State or Federal laws or agreements concerning privacy or security of PII.

**XIV. SIGNATORIES**

The signatories below warrant and represent that they have the competent authority on behalf of their respective agencies to enter into the obligations set forth in this Agreement.

The authorized officials whose signatures appear below have committed their respective agencies to the terms of this Agreement effective this \_\_\_\_\_ day of \_\_\_\_\_, 2012.

For the County of \_\_\_\_\_ Department of Child Support Services:

\_\_\_\_\_  
(Print Name)  
Director

\_\_\_\_\_  
(Signature)

For the California Department of Child Support Services

\_\_\_\_\_  
JUDY RAMOS  
Chief Information Security Officer  
Information Security Office

- Exhibit A: Security and Procedures Manual
- Exhibit B: Confidentiality Statement DCSS Form 0593
- Exhibit C: Security Event Reporting Form (ASD007)

**CONFIDENTIALITY STATEMENT**

DCSS 0593 (03/29/06)

The Department of Child Support Services (DCSS) is responsible for securing Child Support information. DCSS takes this responsibility seriously. The information below describes serious consequences you are subject to in the event that you unlawfully access or disclose Child Support information. Child Support information includes data that is obtained from numerous organizations including, but not limited to: the Internal Revenue Service, the California Franchise Tax Board, the California Employment Development Department, and the California State Board of Equalization. **This information is confidential.** Child Support information also includes DCSS plans, processes, procedures, memoranda, correspondence, research documents, and statistical analysis concerning the DCSS Child Support Program. **This information may be confidential.** Confidential information in any form (e.g. paper, CDs, DVDs, computer drives, mobile computing devices, etc.) is not public and requires special precautions to protect it from wrongful access, use, disclosure, modification, and destruction. DCSS strictly enforces information security. If you violate DCSS confidentiality policies, you may be subject to administrative, civil, and or criminal action.

You may only access confidential information if you have a specific Child Support business need for that information. You may only disclose confidential information to other individuals that have a specific Child Support business need for that information. If you access confidential information without a Child Support business need or if you disclose confidential information to another person that does not have a Child Support business need, you may be subject to discipline by your department, termination of your or your employer's contract, criminal fines, or imprisonment.

- Fines for confidentiality violations range from \$1,000 to \$20,000.
- Imprisonment for confidentiality violations ranges from 1 year to 5 years.
- In addition, you may be liable for damages to persons injured by your confidentiality violation.

By your signature and initials below, you acknowledge that confidential Child Support information is subject to strict confidentiality requirements imposed by state and federal law including, but not limited to: Title 26 United States Code sections 7213(a), 7213A, and 7431; Code of Federal Regulations, Title 28, Code of Federal Regulations, part 603; 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.

***READ AND INITIAL EACH OF THE STATEMENTS PRINTED BELOW***

- \_\_\_\_\_ I acknowledge that operating any computer providing access to Child Support information constitutes consent to monitoring of all system activity. Evidence of unauthorized use collected during monitoring may be used for adverse or criminal action. Logging on to any system providing access to Child Support information indicates acceptance of the DCSS Information Security Policy.
- \_\_\_\_\_ I acknowledge responsibility for knowing the classification of Child Support information. If I do not know the classification of specific information, I will seek classification information from my supervisor.
- \_\_\_\_\_ I 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.
- \_\_\_\_\_ I 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.
- \_\_\_\_\_ I acknowledge that wrongful access, use, modification, or disclosure of confidential information is grounds for immediate termination of my organization's Child Support related contract.
- \_\_\_\_\_ I hereby agree to protect Child Support information in any form, (e.g. paper, CDs, DVDs, computer drives, mobile computing devices, etc) by:
- Accessing Child Support information only as needed to perform my Child Support business duties.
  - Never accessing information for curiosity or personal reasons.
  - Never showing confidential information to or discussion confidential information with anyone who does not have the need to know.
  - Storing confidential information only in approved locations.
  - Never removing sensitive or confidential information from the work site without authorization.
- \_\_\_\_\_ I agree that I will not disclose my password(s) that provide me access to Child Support systems to any other person.
- \_\_\_\_\_ I agree that I will not duplicate or download confidential Child Support information unless I am authorized to do so.

**I certify that I have read and initialed the confidentiality statements printed above.**

\_\_\_\_\_  
PRINT FULL NAME

\_\_\_\_\_  
SIGNATURE

\_\_\_\_\_  
PRINT EMPLOYER'S FULL NAME

\_\_\_\_\_  
DATE

<b>DCSS ISO Use Only</b>	
<b>FTI involved in the incident?</b>	
No	Yes

## DCSS ISO Security Event Report

**Security Event Category** (Both may apply i.e. theft of laptop)

Physical Security  Information Security

Date of Occurrence \_\_\_\_\_ Date Detected \_\_\_\_\_ Location \_\_\_\_\_

**Briefly Describe the Security Event:**

---



---



---

- a. Was crime committed?  No  Yes
- b. Was it reported to law enforcement agency?  No  Yes  
 (Provide copy of police report)

**Additional Information:** (Identify all person(s) involved and their role in the incident.)

Name	Mailing Address	Email	Role (Victim, Suspect or Witness)

**Security Event Reported by:**

Name \_\_\_\_\_ Phone Number \_\_\_\_\_

Division/Unit \_\_\_\_\_ E-mail \_\_\_\_\_

**Security Event Type:**

- a. Threat or act of violence against individual(s) or property. \_\_\_\_ (i.e. bomb threat)
- b. Physical Asset \_\_\_\_\_. (identify below the physical asset(s) involved; i.e stolen laptop)  
 \_\_\_\_\_
- c. Information Asset \_\_\_\_\_ (i.e. child support information)



1. Was personally identifiable information involved?  Yes  No

2. Type of personally identifiable information (Check all that apply)

Name  Social Security Number  Health or Medical Information

Financial Account Number/Access Code  Driver's License/State ID Number

Other (Specify) \_\_\_\_\_

**For DCSS Information Security Office (ISO) Use Only**

**DCSS ISO Classification:**

Security Event \_\_\_\_\_

Security Incident \_\_\_\_\_

Initials \_\_\_\_\_

Initials \_\_\_\_\_

Date \_\_\_\_\_

Date \_\_\_\_\_

**INSTRUCTIONS:** To report a Security Event, call the ISO at (916) 464-5045 or 1-888-327-7435. ISO is available 24 hours a day. If you perceive immediate danger to yourself or to others, please call 911 immediately and then call the ISO.

**How to Submit Event Report:**

An event can be reported by submitting the completed form:

1. By email to [Info.Security@dcss.ca.gov](mailto:Info.Security@dcss.ca.gov) or
2. By calling the ISO at (916) 464-5045 or 1-888-327-7435.

Note: An Event can be reported anonymously by calling the ISO and requesting that the report be treated anonymously.

If you are unsure whether the event or activity you have observed should be reported, call the ISO for assistance at (916) 464-5045 or 1-888-327-7435.