CALIFORNIA DEPARTMENT OF CHILD SUPPORT SERVICES
P.O. Box 419064, Rancho Cordova, CA 95741-9064

May 9, 2008

Reason for this Transmittal

[ ] State Law or Regulation Change
[ ] Federal Law or Regulation Change
[ ] Court Order or Settlement Change
[ ] Clarification requested by One or More Counties
[X] Initiated by DCSS

CSS LETTER: 08-06

ALL IV-D DIRECTORS
ALL COUNTY ADMINISTRATIVE OFFICERS
ALL BOARDS OF SUPERVISORS

SUBJECT: NEW INFORMATION SECURITY MANUAL STANDARD – SEPARATION OF DUTIES

The Department of Child Support Services has added a new standard to the Information Security Manual (ISM). This new standard addresses the requirement for separation of duties to enhance data, system and process integrity by reducing the likelihood of fraud and corruption.

The new standard, attached, is a component of the Asset Protection Policy, and is designated:

2115 Separation of Duties

The ISM is available online from the Information Security Office link on the LCSA Website and from CA Child Support Central:

https://counties.dcss.ca.gov/main/default.asp
https://central.dcss.ca.gov/Pages/Default.aspx

Please contact Debbie Martin, DCSS Chief Information Security Officer at (916) 464-5774 if you have any questions or concerns regarding this matter.

Sincerely,

/os/

DAVID MAXWELL-JOLLY
Director

Attachment: Separation of Duties Standard 2115

Department of Child Support Services

INFORMATION SECURITY MANUAL	NUMBER:	2115
Subject: Separation Of Duties Standard	REVISED DATE:	Original

Section 1: Introduction

Separation of duties segregates duties, responsibilities and tasks of critical/sensitive functions among different individuals. This standard is intended to enhance data, system and process integrity by early detection and prevention of fraud, corruption and/or other inappropriate activities.

Section 2: This standard focuses primarily on mechanisms implemented through processes and procedures that compliment system enforced controls.

2.1 Separation of Duties Requirements

Applicable Organizations must:

1. Define roles and responsibilities associated for all positions (staff, managers, supervisors, security personnel, etc.).
2. Analyze each position to assure that no one person is given excessive authority or job responsibility to carry out tasks that may result in inappropriate activities or misuse of authority, for example: fraud, theft or embezzlement.
3. Implement controls that divide functions so that no one person has inappropriate authority over multiple parts of a transaction. The following practices are recommended to prevent adverse impact (inadvertent or intentional) to Child Support Information and IT Assets:
    - Development staff should not have access to production systems and data bases.
    - Procurement functions must be segregated. Staff that solicit bids or made recommendations for selection must not review and approve the selection.
    - Purchasing functions must be segregated. Staff that submits orders for goods and services must not review and approve the purchase orders.
    - Master files changes must be authorized and initiated by persons independent of the data processing function.[1]
    - Any override capability or bypassing of data validation on editing problems must be restricted to supervisory personnel.[2]
    - Adjustments to previously processed payments should require supervisory approval.[3]
    - Child Support financial workers must not perform case management functions such as case opening and participant creation.

[1] Automated Systems for Child Support Enforcement: A Guide for States, August 2000, Requirement H-4a

[2] Ibid, requirement H-4b

[3] Ibid, requirement F-2d

4. Periodically assess functional capabilities against staff's assigned duties to ensure enhanced security. For example, individual's privileges and authorities should be reviewed for appropriateness upon change of staff duties.
5. Ensure that the users are granted the minimum level of access to perform their duties.
6. Develop and communicate process and procedures to report violations in accordance with DCSS ISM 3100 Security Incident Management Standard.
7. Educate staff to identify and report potential conflicts between duties, responsibilities and authorities.

Section 3: Enforcement, Auditing, Reporting

1. Violation of this policy may result in disciplinary action that may include termination for employees and temporaries; termination of employment relations in the case of contractors or consultants; or dismissal for student assistants. Additionally, individuals may be subject to loss of Child Support Information access privileges, and if warranted, civil, or criminal prosecution under California or federal law.
2. DCSS is responsible for the periodic auditing and reporting of compliance with this policy. DCSS will define the format and frequency of the reporting requirements and communicate those requirements, in writing, to Applicable Organizations. In addition, DCSS Management can conduct an ad hoc audit at any time.
3. Exceptions to this policy will be considered only when the requested exception is documented using the DCSS ISM 1200 Exception Handling Procedure and submitted to the DCSS CISO.
4. Any person may, at any time, anonymously report policy violations by telephone at (916) 464-5045 or by email to Info.Security@dcss.ca.gov.

Section 4: References

1200- Exceptions Handling Process

3100 – Security Incident Management Standard

2000 - Asset Protection Policy

U.S Department of Health and Human Services/ ACF, Automated System for Child Support Enforcement: A Guide for States, August 2000

Safeguards for protecting Federal Tax Return and Return Information; Publication 1075, February 2007; p. 78; Separation of Duties

Section 5: Control and Maintenance

Policy Version: 1.0

Date: May 9, 2008

Owner: DCSS Information Security Office