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

September 24, 2009

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: 09-02

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

SUBJECT: NEW INFORMATION SECURITY STANDARDS AND REVISIONS TO THE INFORMATION SECURITY MANUAL

The Department of Child Support Services (DCSS) has added two additional standards to the Information Security Manual (ISM) and has made revisions to existing policy and standards to meet additional requirements and to provide clarification.

The revisions to existing ISM policies and standards are outlined in the attached ISM Record of Changes. The new standards, attached, are components of the Asset Protection Policy.

2108 Physical Security Standard
2109 Secure Data Transfer Standard

The ISM and supporting guidelines, forms, and templates, including sample security contract language, are available online from the Information Security link on the California Child Support Central website.

https://central2.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 these additions or changes.

Sincerely,

Mary Ann Miller
Assistant Director

Attachment: ISM Record of Changes
2108 Physical Security Standard
2109 Secure Data Transfer Standard

California Department of
Child Support Services

Information Security Manual

Record of Changes

September 2009

ISM Section	Action Type	Description of Changes
Global	Revised	Changed the reference from the U.S. Department of Health and Human Services/ACF, Automated System for Child Support Enforcement: A Guide for States, June 2000 to June 2007.
Global	Revised	Changed applicable State Administrative Manual (SAM) policy references and added National Institute of Standards and Technology (NIST) Special Publication (SP) references.
Global	Revised	Changed references for ISM 3200 Security Incident Procedures to ISM 3100 Security Incident Management Standard.
1000	Revised	Changed Introduction to an overarching Information Security 'Policy' for the DCSS Information Security Program referencing additional state and federal laws and standards. Removed the numbering system guideline and replaced the Annual Certification Compliance requirement with compliance visits by the DCSS ISO within a three-year cycle.
1310	Removed	The Annual Certification Requirement Form is replaced with the DCSS ISO compliance visits.
2100	Revised	Changed Access Control Standard language for Logon Banners and Warning Notices to a higher level requirement for flexibility to customize system warning language with applicable laws and policies appropriate for the system.
2108	New	Added new standard for Physical Security to comply with SAM 5330; IRS P1075 section 4, Secure Storage; and NIST SP 800-53, Physical and Environmental Protection.
2109	New	Added new standard for Secure Data Transfer to comply with IRS P1075; and NIST SP 800-53, Transmission Integrity, and Transmission Confidentiality.
2115	Revised	Separation of Duties revised to correct formatting.
3300	Removed	The Security Event Report Form, ASD007, replaces ISM 3300 and is available from the CA Child Support Central website.
3100	Revised	Changed reference within Security Incident Management Standard from ISM 3300 Security Incident Reporting Form to ASD007, Security Event Report Form. Added key terms and definitions for clarity. Removed reference to 888-DCSS-HELP (888-327-7435) telephone number. This number will be eliminated in the future.
5000	Revised	Acceptable Use Policy revised to comply with IRS P1075 and NIST SP 800-53 prohibiting the installation of unlicensed software and violations of copyright laws; installation of personally-owned copies of software (including peer-to-peer file sharing software); and connecting personally-owned information management devices to Child Support IT Assets.
7000	Revised	Risk Management Policy updated to reflect IRS P1075, SAM, and NIST SP 800-53 requirements to address documented Security Plans and security controls reviews and assessment as part of the Risk Management process.

Department of Child Support Services

INFORMATION SECURITY MANUAL	NUMBER:	2108
Subject: Physical Security Standard	**REVISED DATE:**	**Original**

Section 1: Introduction

The objective of physical security is to secure and monitor facilities containing Child Support Information and Child Support IT Assets to prevent intentional or unintentional damages due to natural or unnatural causes. Physical security includes workplace processes, procedures, and preventive measures designed to protect the confidentiality, integrity and availability of Child Support Information. For the purpose of this standard, the term "facilities" means any building in which Child Support Information is processed or stored. See ISM 3100, Security Incident Management Standard, for security incident reporting requirements, including physical security. This standard includes:

- Facility Security
- Work Area Security

Section 2: Standard Directives

2.1 Facility Security

To ensure the protection of Child Support Information, the facilities should be strategically located and the building and the work site must be protected in a manner that minimizes the risk of crime, theft, destruction and unauthorized access.

2.1.1 Facility Site Selection Requirements

Applicable Organizations must:

1. When selecting a site for a facility to process or store Child Support Information and Child Support IT Assets, conduct a risk analysis to determine potential physical threats to each site being considered. Threats to be included in the risk assessment must include, at a minimum, earthquake, flood, fire, power failure, and physical intrusion. The criteria for site selection must consider the relative risks to Child Support Information and Child Support IT Assets for each site being considered.
2. When selecting a vendor to provide offsite services that process or store Child Support Information such as printing, scanning, storage, computer services, money collection and disbursement, the procurement evaluation must include facility and location risks in selecting the prospective vendor. The vendor should be required to provide a risk analysis of the proposed site that includes earthquake, flood, fire, power failure, physical intrusion and other risk factors relevant to the site's environment.

2.1.2 Perimeter Security Requirements

Applicable Organizations must use security perimeters (barriers such as walls, card controlled entry gates, security guards or staffed reception desks) to restrict access to facilities or areas within facilities that process or store Child Support Information or contain Child Support IT Assets. The following measures must be implemented for physical security perimeters:

1. Conduct a risk assessment to determine the appropriate procedures and controls necessary to prevent unauthorized intrusion to restricted areas. At a minimum the risk assessment must consider location, number, type and strength of perimeters.

2. Implement multiple barriers of physical protection to ensure that failure of one physical barrier will not immediately compromise the restricted area. (For example: secured perimeter/locked container; locked perimeter/secured interior; or locked perimeter/security container.) [1]
3. Clearly define and control security perimeters.
4. Document and implement processes and procedures to ensure that perimeters prevent pubic access to the areas used to process and store Child Support Information and Child Support IT Assets.
5. Document and implement processes and procedures to ensure that perimeters are physically sound (i.e. there should be no gaps in the perimeter walls, floors and ceilings where a break-in could easily occur).
6. Control entrances and exits through perimeters to restrict access to authorized Child Support Employees. Controls include security revolving doors, locking mechanisms with assigned keys, badges, codes or biometric controls, manned reception areas, video monitoring, etc. At a minimum, there must be a means to log the entrance of personnel through perimeters.
7. Establish internal perimeters between entities when sharing a facility with another entity.
8. Ensure all fire doors on a perimeter are alarmed and monitored.
9. Document and implement processes and procedures to test intrusion detection devices. Procedures must include test frequency.
10. Document and implement procedures to ensure loading docks are protecting Child Support IT Assets from unauthorized exposure.
11. Restrict signage and logos on facilities supporting data centers, back up data storage sites, operational recovery sites to ensure that the facilities are not identified as child support facilities.

2.1.3 Public Area Security

Public area security covers both public areas and public service areas. These distinct areas are defined as:

1. A public area is an unrestricted area in any of the Applicable Organization's facility which is not a place to provide services to general public. An example of a public area is a lobby of one of the Department of Child Support Services buildings that allows unrestricted access to individuals that are not employed by the Applicable Organization. Security of such area must be assessed and managed in proportion to the risk.
2. A public service area is an area where members of the general public are invited or directed to conduct business with the applicable organization. An example of a public service area is a public counter at a local child support agency or lobby of a facility containing a self-service kiosk. The following minimum controls must be implemented to secure public service areas:
   a. Access to public service areas must be restricted to established business hours.
   b. Public service areas must be monitored by Child Support Employees, security guards, or video cameras.
   c. Self service kiosks in public service areas must be configured to ensure that only intended kiosk users are able to access the information those users are authorized to access.
   d. Public service areas must contain a mechanism (emergency telephone, alarm button) to facilitate immediate notification of security guards or police to report threats to persons or property.

---

[1] IRS Publication 1075, section 4.2, Minimum Protection Standards (MPS)

2.1.4 Facility Security Processes and Procedures

To ensure security of facilities and availability of child support services, Applicable Organizations must document and implement the following procedures at a minimum:

1. Risk assessment procedures which include a schedule for conducting periodic risk assessments of facilities as it relates to the protection of Child Support Information and Child Support IT Assets.
2. Incident reporting and response procedures for incidents involving facilities that fail to prevent theft loss, damage, and unauthorized modification, release, or access to Child Support Information or Child Support IT Assets, or interruption of child support services.
3. Business continuity responsibilities relating to facilities, including contact and coordination with Applicable Organizations' facilities and procurement personnel.
4. Documentation and implementation of emergency reporting and response procedures.
5. Facility access procedures for visitors and vendors (such as, copy machine technicians, vending machine suppliers, etc.) that track, monitor, and control access to restricted areas. For example: visitor logs, visitor identification (badges), Child Support Employee escort, and security personnel notification of unidentified or unescorted visitors.
6. Procedures for managing Child Support Employees' access to facilities must include:
   a. Authorize and document Child Support Employees' access to facilities.
   b. Require management approval for access to areas within facilities that require additional access controls, e.g. server room, Human Resources or work area for sensitive processes.
   c. Deactivate access of Child Support Employees upon termination of employment or contract term.
   d. Review and audit Child Support Employees' access to facilities.

2.2 Work Area Security

A work area is defined as the area used for processing or storing Child Support Information and Child Support IT Assets. Access to these areas is restricted to those employees who have a business need. Applicable Organizations must implement the following to facilitate security within the work area:

1. Train Child Support Employees regarding the existence of and importance of physical premises and physical access rules to enable them to help identify and report the presence of unauthorized persons within restricted areas.
2. Train employees to report unexpected objects in work areas.
3. Restrict the use of recording features (i.e., video, audio) on recording devices such as cameras, cell phones, or other recording equipment, in restricted areas unless specifically authorized.
4. Inspect facilities periodically to check for unexpected and unauthorized property or activities.
5. Develop policies and procedures to assure Child Support Information is not left exposed or unattended when leaving the work area.
6. Implement process and procedures to control removal of Child Support Information from the work area. For example: employees cannot take work related information home or other places outside the work area without management approval.
7. Place and position equipment so as to minimize disclosure of confidential and personal information to unauthorized individual(s). For example, computer monitors, printers, and FAX machines that process confidential and personal information should not be installed in high traffic areas which are frequented by persons with no need to know such information.

8. Protect documents containing Child Support Information in storage to minimize exposure of confidential, personal and sensitive information to unauthorized individuals.

Section 3: Enforcement, Auditing, and 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 1300 Information Security Exception Request Form 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: Related Policies and Standards

ISM 1200 – Exception Handling Process and Form

ISM 2000 – Asset Protection Policy

ISM 2103 – Information and IT Asset Classification Standard

ISM 3100 – Security Incident Management Standard

Section 5: References

SAM Section 5330 – Physical and Environmental Security

U.S. Department of Health & Human Services/ACF, Automated System for Child Support Enforcement: A Guide for States, June 2007, H-1c

Section 6: Control and Maintenance

Date Issued: September 24, 2009

Owner: DCSS Information Security Office

Version: 1.0

Department of Child Support Services

INFORMATION SECURITY MANUAL	NUMBER:	2109
Subject: Secure Data Transfer Standard	**REVISED DATE**	**Original**

Section 1: Introduction

Child Support Information must be used for its intended purpose only, and must be protected when not in the direct management and control of the Applicable Organization. This standard addresses the security requirements for transferring confidential and personal Child Support Information to an external entity as a result of a data sharing or exchange agreement, such as a contract, inter-agency agreement (IAA), memorandum of understanding (MOU), service level agreement (SLA), or other binding form or document. Standard directives include the following:

- Information Owner Requirements
- Data Transfer Agreement Requirements
- Information Custodian Requirements

Section 2: Key Terms and Definitions Applicable to this Standard

Personal Information – Any information classified as personal in accordance with ISM 2103, Information and IT Asset Classification. Examples include, but not limited to, Child Support records containing participant's name and social security number; Child Support Participant bank account number and access code; Child Support Employee data that contain employee's name and California driver's license number or social security number; and family violence participant data.

Confidential Information – Any information classified as confidential in accordance with ISM 2103, Information and IT Asset Classification. Examples include, but not limited to, Child Support Participant application for child support services; records pertaining to pending litigation or claim; medical records; documents protected by attorney-client privilege; home addresses and home telephone numbers of employees; and Federal Tax Information (FTI). E-mail may not be used to transfer *FTI*.

Data – Child Support Information classified as personal or confidential.

Security Boundary – All the components that establish controls to monitor and control the flow of information within and at the external boundary of the information system and networks of an Applicable Organization with direct management control and security support structure.

Data Transfer – The act or process of moving personal or confidential data on either electronic (e.g., via network, email, application, facsimile, etc.), or physical (e.g., via CD, USB flash drive, paper document, etc.) medium outside the physical or network security boundaries of an Applicable Organization as the result of a data sharing or exchange agreement.

Federal Tax Information – Any federal tax return or return information received from the Internal Revenue Service as the originating source either directly or indirectly.

Information Owner – An Applicable Organization that classifies and secures Child Support Information for which they are responsible. This may be the California State Department of Child Support Services (DCSS) or local child support agency (LCSA).

External Entity – Any public or private organization outside the physical or network security boundary of an Applicable Organization.

Information Custodian – An individual, organization or subunit (e.g., DCSS, LCSA, or external entity) that has delegated responsibility for handling and maintaining the security of Child Support Information while in their custody.

Section 3: Standard Directives

All data transfers to an external entity require an approved agreement be in place prior to commencing data transfer. Approved agreements can be contracts, inter-agency agreements (IAAs), memorandum of understanding (MOUs), service level agreements (SLAs), or other binding forms or documents.)

3.1 Information Owner Requirements

Applicable Organizations that are the Information Owner must:

1. Review requested data transfers and ensure they are necessary for legitimate business purposes.
2. Identify the external entity to which Child Support Information is to be transferred.
3. Identify the data source (e.g., physical location, system or application, etc.).
4. Identify the method of transferring the data.
5. Identify how long external entity shall retain the data sent to them.
6. Identify security and privacy risks of data prior to approving data transfer.
7. Consider security measures of external entities as a key component of evaluation and selection for acquiring an external entity to provide services or support for data transfers.
8. Ensure data sharing or exchange agreements include defined requirements for processes and procedures for security protection measures for meeting acceptable levels of data security and privacy protection prior to transferring data.
9. Ensure external entity has a contractual agreement or other binding form or documents with Applicable Organization in accordance with section 3.2 of this standard.
10. Require external parties to return all Child Support Information or certify in writing of the destruction of all Child Support Information when they are no longer needed for the business purpose for which they were obtained or agreed upon period of time of data retention or termination of agreement.

3.2 Data Transfer Agreement Requirements

External entities must develop and implement security measures (management, operational, and technical) to ensure that they provide the same level of protection to the data transferred to them as is provided by the Information Owner. Agreements with an external entity must consider, at minimum, the following contractual security elements:

1. Policies and procedures. Policies and procedures must be implemented to protect data in accordance with applicable federal and state laws and consistent with the DCSS ISM.
2. Use of information. Child Support Information must be used solely for the purposes specifically authorized under the agreement. Any other use of Child Support Information is strictly prohibited.
3. Method of data transfer. Child Support Information must be encrypted when transmitted over a public network in accordance with ISM 2111, Encryption.
4. Access to information. Child Support Information must be protected against unauthorized or unlawful access to and against accidental loss or destruction with identification and access control measures consistent with ISM 2000, Asset Protection and associated standards.

5. Unique identification. The use of unique individual user identifier and user-selected password for each person utilizing each system capable of accessing Child Support Information must be implemented in accordance with ISM 2100, Access Control.
6. Security awareness training. Annual security awareness training must be given to all individuals that access or support Child Support Information pursuant to the agreement and consistent with ISM 6000 Security Awareness.
7. Statement of confidentiality. Signed confidentiality statements must be obtained annually in accordance with ISM 6000, Security Awareness and retained for a period of three (3) years.
8. Access authorization records. All access to transferred Child Support Information must be recorded and access records maintained for six (6) years. These records must be made available to the Information Owner's Applicable Organization upon request.
9. Inspection. Applicable Organization must have the right to send its officers and employees into the office and plants of the external entity for assessment in accordance with ISM 7000, Risk Management of the facilities and operations provided for the performance of the work under the agreement.
10. Destruction of records. All data obtained during the performance of the agreement must be returned or destroyed with written certification when they are no longer needed for the business purpose for which they were obtained.
11. Incident management. Known or suspected security incidents consistent with ISM 3100, Security Incident Management must be reported to the DCSS ISO. This includes reporting data suspected to be lost during transfer. External entities must cooperate with DCSS and/or Information Owner's Applicable Organization in any investigations of incidents involving Child Support Information.
12. Secure areas. Computer monitors, printers, hard copy printouts or any other forms of information accessed or obtained under the performance of the agreement must be placed so that they may not be viewed by the public or other unauthorized persons as described in the agreement.
13. Secure storage. Information in all forms, such as but not limited to tapes, cartridges, or other removable media, must be stored in areas physically secure from access by unauthorized persons.
14. Media protection. All portable media, excluding backup media, used to store Child Support Information, such as but not limited to portable computing devices, CDs, DVDs, USB flash drives, tapes, and cartridges must be encrypted in accordance with ISM 2111, Encryption.
15. Change Management. All changes to computer systems, hardware, software, applications, storage media, and network components used for storing and/or accessing information in the performance of the agreement must be consistent with ISM 4100, Configuration Management.
16. Monitoring. An audit trail and record of data access of authorized users and authorization level of access granted to information, based on job function must be maintained in accordance with ISM 2100, Access Control.
17. Screen-locking. Computers capable of accessing information for the performance of the agreement must not be left unattended and logged on, unless secured by a screen-locking process or mechanism in accordance with ISM 2100, Access Control, or physically secured in ISM 2108, Physical Security.

3.3 Information Custodian Requirements

Child Support Information Custodian must maintain the security and confidentiality of Child Support Information and ensure the implementation of security controls prescribed by the Information Owner. Child Support Information Custodians must ensure:

1. Data transfers have prior written approval by Applicable Organization's Information Owner.
2. Data transfers have prior approval from Applicable Organization's information security officer.

3. All electronic Child Support Information transferred to an external entity uses methods of encryption in accordance with ISM 2111, Encryption. This includes data transfers via the use of email, FTP or any portable storage media (e.g., CD, DVD, USB flash drive, etc.).
4. A method is in place to terminate data transfers.
5. The use of fax machines to transmit data is avoided whenever possible. Multiple layers of security mechanisms must be in place to ensure accurate sending and receipt of transferred data. (Examples include but not limited to the use of a fax cover sheet with a statement of the confidentiality of the data, the need for protection, and notice to unintended recipients to telephone the sender; ensuring trusted personnel are located at both the sending and receiving fax machines; and validating receipt of the fax by contacting external entity, etc.).
6. Ensure receipt of data transferred.
7. Records or logs that document the data transfer must be retained and made available to the DCSS ISO for up to six (6) years. Documentation or records must include information that verifies what data was transferred, the destination of the data, and acknowledgement of receipt of data.
8. Automated data transfers that run without manual interventions whatsoever other than to start the automated transfer process have a termination date.
9. An action plan for notification for any information security breach involving Child Support Information is in place in accordance with ISM 3100, Security Incident Management.

Section 4: Enforcement, Auditing, and 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 1300 Information Security Exception Request Form 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 5: Related Policies and Standards

ISM 2000 – Asset Protection Policy

ISM 2100 – Access Control

ISM 2103 – Information and IT Asset Classification Standard

ISM 2111 – Encryption Standard

ISM 3100 – Security Incident Management Standard

Section 6: References

SAM Section 5320.2 – Responsibility of Owners of Information

SAM Section 5320.3 – Responsibility of Custodians of Information

SAM Section 5345.2 – Cryptography

P1075, IRS Safeguards for Protection Federal Tax Returns and Return Information – Sections 3.2 Electronic Files; 3.3 Non-electronic Files; 5.6.2 Audit and Accountability; and 6.3.1 Record Keeping

U.S. Department of Health and Human Services/ACF, Automated System for Child Support Enforcement: A Guide for States, June 2007

National Institute of Standards and Technology (NIST) Special Publication 800-47

Section 7: Control and Maintenance

Date Issued: September 24, 2009

Owner: DCSS Information Security Office

Version: 1.0