Information Security Manual

Supporting California's Children

May 2010

Information Security Office
California Department of Child Support Services

THIS PAGE IS INTENTIONALLY LEFT BLANK

California Department of
Child Support Services

Information Security Manual

Record of Changes

May 2010

Subject	Section	Action Type	Description of Changes
Access Control	2100	Revised	Changed 2.3.4 #1 automatic lock for workstations to 10 minutes of inactivity from 15 minutes. This change meets DMV access requirements for access to DMV information.
Access Control	2100	New	Added language 2.3.4 #2 to address IRS requirements for network session termination to be at 15 minutes or less and make reference to ISM 2104 for mobile computing devices.
Passwords	2101	Revised	Reworded and revised 2.2 #12 to eliminate the requirement to encrypt email that include passwords and clearly identified that user ID not be included together in an email with a password. Revised 2.2 #11 to clarify that it's 'okay' for passwords to be stored electronically in encrypted files.
Mobile Computing	2104	Revised	Added language 2.1 #4 to refer to ISM 2100 Access Control, and reworded 2.1 #5 for clarification adding reference to ISM 2111 Encryption.
Media Protection and Sanitation	2110	New	Added standard for media protection and handling to comply with media protection areas of the IRS Publication 1075, State Administrative Manual, and NIST 800-53.
Systems Acquisition, Development and Maintenance	2112	New	Added new standard for DCSS acquisitions, development, and maintenance of DCSS systems and assets.
Secure System	2105	Revised	Added 2.1 #5 to address separation of system user functionality from administrative functionality. Added 2.1 #6 requiring system design to prevent unauthorized or unintended transfer of information via shared system resources. (Refer to NIST SP 800-53 SC-2 and SC-3; and IRS P1075 5.6.15). Added 2.2.2 #6 additional event log management requirements to Secure Systems Standard.
Incident Management	3100	Revised	Revised 3.1 for clarification from establishing and maintaining procedures to establishing incident response procedures; and revised 3.2 for clarification from incident reporting requirements to criteria for reporting incidents.

THIS PAGE IS INTENTIONALLY LEFT BLANK

DCSS Information Security Manual

Table of Contents

Information Security Policy **1000**
ISM Exception Handling Procedure 1200
ISM Definitions 1301
Asset Protection Policy **2000**
Access Control Standard 2100
Password Standard 2101
Remote Access Standard 2102
Information and IT Asset Classification Standard 2103
Mobile Computing Device Standard 2104
Secure System Standard 2105
Conflict Recusal Standard 2107
Physical Security Standard 2108
Secure Data Transfer Standard 2109
Media Protection and Sanitation Standard 2110
Encryption Standard 2111
Systems Acquisition, Development and Maintenance 2112
Wireless Communication Standard 2114
Separation of Duties Standard 2115
Threat Management Policy **3000**
Security Incident Management Standard 3100
Disaster Recovery Standard 3101
Virus Management Standard 3102
Vulnerability Management Policy **4000**
Configuration Management Standard 4100
Patch Management Standard 4101
Acceptable Use Policy **5000**
Security Awareness Policy **6000**
Risk Management Policy **7000**
Appendices
Exception Request Form – DCSS ISM 1300
DCSS ISO Security Event Report Form – ASD700

Alphabetical Order

DCSS Information Security Manual

Table of Contents

Acceptable Use Policy 5000
Access Control Standard 2100
Asset Protection Policy 2000
Configuration Management Standard 4100
Conflict Recusal Standard 2107
Definitions 1301
Disaster Recovery Standard 3101
Encryption Standard 2111
Exception Handling Procedure 1200
Information and IT Asset Classification Standard 2103
Information Security Policy 1000
Media Protection and Sanitation Standard 2110
Mobile Computing Device Standard 2104
Password Standard 2101
Patch Management Standard 4101
Physical Security Standard 2108
Remote Access Standard 2102
Risk Management Policy 7000
Secure Data Transfer Standard 2109
Secure System Standard 2105
Security Awareness Policy 6000
Security Incident Management Standard 3100
Separation of Duties Standard 2115
Systems Acquisition, Development and Maintenance 2112
Threat Management Policy 3000
Wireless Communication Standard 2114
Virus Management Standard 3102
Vulnerability Management Policy 4000
Appendices
DCSS ISO Security Event Report Form – ASD700
Exception Request Form – DCSS ISM 1300ISM References

Department of Child Support Services

INFORMATION SECURITY MANUAL	NUMBER:	1000
Subject: Information Security Policy	**REVISED DATE:**	**09/24/2009**

Section 1: Introduction

The mission of the California Child Support Program is to promote the well-being of children and the self-sufficiency of families by delivering quality child support establishment, collection, and distribution services that help both parents to meet the financial, medical, and emotional needs of their children. The purpose of this policy is to establish information security requirements in accordance with state and federal law in support of Department of Child Support Services (DCSS) and its administration of the California Child Support Program.

California Child Support Information and Child Support IT Assets are valuable assets that must be protected. This policy demonstrates the commitment of Child Support Program management and establishes the requirement to create, maintain, and adhere to a uniform set of information security policies, standards, and guidelines.

Section 2: Roles and Responsibilities

1. DCSS Management will establish a periodic reporting requirement for the DCSS Chief Information Security Officer (CISO) to measure the compliance and effectiveness of DCSS Information Security Manual (ISM) policies and standards.
2. Applicable Organizations' Management will be responsible for implementing the requirements of DCSS ISM policies and standards.
3. Applicable Organizations' Management, in cooperation with the DCSS CISO, is required to train employees on DCSS ISM policies and standards.
4. Child Support Employees will comply with DCSS ISM policies and standards.

Section 3: Policy Directives

In accordance with the California State Administrative Manual (SAM) Section 5100 and the Internal Revenue Services (IRS) Publican 1075, Safeguards for Protecting Federal Tax Return and Return Information, the DCSS ISO shall create information security policies, standards, and guidelines based upon the American National Standards Institute management information standards and the Federal Information Processing Standards. These shall facilitate an information security infrastructure based on the risk management framework established by the Federal Information Security Management Act (FISMA) of 2002 and the supporting documentation developed by the National Institute of Standards and Technology (NIST) that protect the integrity, confidentiality, and availability of its information assets from unauthorized disclosure, modification, use, or destruction, while still meeting business objectives.

3.1 DCSS Information Security Office

DCSS recognizes and acknowledges that information assets are the foundation of the California Child Support Program and must be secured to ensure that the organization's mission is achieved. Consequently, the DCSS Director has appointed the DCSS CISO to manage the DCSS Information Security Office (ISO) and the Information Security Program. The CISO has delegated authority to implement appropriate oversight and assurance procedures to ensure Child Support Employees and Applicable Organizations comply with Information Security Program requirements.

The DCSS ISO acts as the independent information security oversight organization and has information security authority for all California Child Support Information, IT Assets, business processes, and personnel. The goal of the DCSS ISO is to ensure that the appropriate security controls are in place to protect Child Support Information and Child Support IT Assets from the risk of accidental or intentional interruption of service as well as unauthorized access, disclosure, modification, or destruction of information assets.

3.2 DCSS Information Security Program

The DCSS Director approves, sponsors, and supports the Information Security Program and has established the ISO which is responsible for the development, implementation, maintenance, and enforcement of the *Information Security Program*.

The objective of Information Security is the preservation of:

- confidentiality: preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information;
- integrity: guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity;
- availability: ensuring timely and reliable access to and use of information.[1]

3.3 Information Security Manual

The DCSS ISM is produced for use by all individuals having access or responsibility to manage California Child Support Information and Child Support IT Assets. The term "Applicable Organization" appears throughout the DCSS ISM. Applicable Organization refers to any organization whose employees or contractors may have access to Child Support Information or Child Support IT Assets. Another term used throughout the manual is "Child Support Employee." Child Support Employee means an employer or contractor that may have access to Child Support Information or Child Support IT Assets due to his or her employment by any Applicable Organization. Terms defined specifically for the DCSS ISM, can be found in ISM 1301 Definitions. These terms apply to all sections of the DCSS ISM. All defined words throughout the DCSS ISM are capitalized.

The DCSS ISM structure is hierarchal, with policies at the top. Each policy contains mandatory directives and assigns roles and responsibilities for carrying out the directives.

---

[1] 44 U.S.C., Sec. 3542

- **Policies** – Description of the overall framework or high-level statements of direction, purpose, principles, or method for managing and implementing information security.
- **Standards** – More detailed mandatory directives of prescribed specifications, approach, solution, methodology, or protocol that must be followed.
- **Guidelines** – Recommended course of actions or tasks for meeting specific principles or directives, but are not mandatory.

Section 4: Enforcement, Auditing, and Reporting

1. The DCSS ISM applies to all Information, Information Systems, IT Assets, and business processes that are used in support of the California Child Support Program. All individuals having access to Child Support Information and IT Assets are required to comply with the DCSS ISM. Compliance with the ISM is mandatory to ensure a consistent and strategic approach to protect information and IT assets.

   The DCSS ISM does not apply to systems or information that is used for purposes other than the support or administration of the California Child Support Program.

2. Compliance with the DCSS ISM will be verified during reviews conducted by the DCSS ISO at minimum within a three-year cycle. California Child Support Program organizations are required to evaluate their processes and systems and if necessary, implement additional protection mechanisms to adequately protect California Child Support Information and IT Assets.
3. Recognizing that some business processes and/or technical environments will prevent full compliance with the DCSS ISM, policy exceptions 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.

Section 5: References

SAM Chapter 5300 – Information Security and Privacy Protection

IRS Publication 1075 – Safeguards for Protecting Federal Tax Return and Return Information

NIST Special Publication 800-53 – Recommended Security Controls for Federal Information Systems and Organizations

Section 6: Control and Maintenance

Date Issued: January 16, 2007

Owner: DCSS Information Security Office

Version: 2.0

Department of Child Support Services

INFORMATION SECURITY MANUAL	NUMBER:	1200
Subject: Exception Handling Procedure	**REVISED DATE:**	**09/24/2009**

Section 1: Introduction

DCSS Information Security policies and standards are developed and implemented to best protect Child Support Information and Child Support IT Assets. Exceptions to the policies may increase security risks yet may be justified under certain circumstances. The purpose of this exception process is to ensure that all exceptions from DCSS information security policies and standards are assessed for potential security risks and that mitigation strategies are implemented where appropriate. Applicable Organizations' Management or Child Support Information/IT Asset Owner may request an exception pursuant to this procedure. The purpose of this procedure is to provide instructions on how to request exceptions to policies and standards established in the DCSS ISM.

Section 2: Procedure Directives

2.1 Requesting an Exception

To request an exception to a DCSS ISM policy or standard, the manager of the Applicable Organization or the Child Support Information or IT Asset Owner will complete the ISM 1300 Exception Request Form and submit it to the DCSS CISO. The following items must be completed on the form:

1. The name and number of the DCSS ISM policy or standard for which the exception is requested. Requests for Exception to multiple policies and/or procedures may be submitted as a single request when there is a common underlying reason.
2. The length of time for which the exception(s) are requested.
3. Date when exception is necessary.
4. The scope of the requested exception(s):
   a. organization unit to which the exception(s) will apply (for example, will the exception apply to the entire Applicable Organization or to specific working units within the organization).
   b. persons to which the exception(s) will apply (for example, will the exception apply to the entire Applicable Organization or a specific unit or individuals).
   c. physical location(s) to which the exception(s) will apply.
5. A description of the technical or business need for each requested exception. This should be a detailed explanation of what the exception entails. Include a description of:
   a. how the identified DCSS ISM policy or standard would be modified for scope described above.
   b. the business process or technical need for this modification.

c. the impact on business processes, system functionality or technical quality, if the exception is not allowed.

d. any costs that may be incurred if the exception is not approved.

e. any security risk to Child Support Information IT assets that may arise, if the exception is approved.

f. all mitigation actions that may be taken to reduce the security risks described in "e" above.

6. The name, title and contact information for the contact person for questions regarding the request.

7. Signature of individual responsible for requesting the Exception.

2.2 Reviewing Request for Exception

The DCSS CISO or designee will review the request for exception, and will assess the needs and impacts of the requested exception. The DCSS CISO will consult with subject matter experts including the Chief Information Officer of the requesting entity as appropriate to verify the impacts, costs, risks and mitigation actions.

2.3 Action on Request for Exception

The DCSS CISO will approve or disapprove the Exception request.

2.4 Documentation

The DCSS CISO will track requests for exceptions, actions on the requests and will retain related documentation. The DCSS CISO will establish the appropriate retention period for these materials.

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 1000 – Information Security Policy

ISM 2000 – Asset Protection

Section 5: References

SAM Chapter 5300 – Information Security (Office of Information Security and Privacy Protection)

Section 6: Control and Maintenance

Date: January 16, 2007

Owner: DCSS Information Security Office

Version: 2.0

Department of Child Support Services

INFORMATION SECURITY MANUAL	NUMBER:	1301
Subject: DCSS ISM Definitions	REVISED DATE:	Original

Section 1: Introduction

The following terms apply to all sections of this DCSS Information Security Manual. Defined terms will be capitalized throughout the manual.

Section 2: Definitions

Term	Definition
Applicable Organization	Any organization whose employees or contractors may have access to Child Support Information or Child Support IT Assets containing Child Support Information.
Applicable Organizations' Management	Includes DCSS Management and comparable level managers for each of the Applicable Organizations
Child Support Employee	An employee or contractor that works for any Applicable Organization that may have access to Child Support Information or Child Support IT Assets.
Child Support Information	Information, whether in the form of electronic media, physical document; data originated, taken or summarized from Child Support systems including all data maintained or accessed through Child Support systems owned or administered by or on the behalf of the Child Support Program.
Child Support IT Assets	The hardware, software, including system and application software, and the network and communication components that are used to process and store Child Support Information.
Child Support Participant	A custodial party, a non custodial parent, or a dependent in a child support case.
Critical	Critical is the term used to classify Child Support IT Assets and business processes that are essential to achieving Child Support Service's mission.
DCSS CISO	The Chief Information Security Officer for the Department of Child Support Services
DCSS Management	Includes Department of Child Support Services executive managers and DCSS branch managers

Term	Definition
Child Support Information/IT Asset Custodian	The individual, organization or subunit (typically IT function) that is delegated the responsibility for handling and safekeeping of Child Support Information and Child Support IT Assets while in their custody. The Data custodian has the responsibility to: • Assist Information/IT Asset Owners with maintaining the confidentiality, integrity, and availability of their information and data. • Assist Information/IT Asset Owners with implementing the prescribed technical security controls. • Monitor IT assets and immediately report security breaches to the Information/IT Asset Owners and the CISO.
Child Support Information/IT Asset Owner	The Applicable Organization or its organizational subunit which is assigned ownership of data file or database or a Child Support IT Asset. This responsibility mostly belongs in the business units. Information/IT Asset Owners are responsible for protecting the confidentiality, integrity and availability of assets under their ownership.
System	A System refers to a collection of processes, hardware, network, communication structure and software associated with Child Support Services; i.e. databases, operating system etc.

Section 3: Control and Maintenance

Owner: DCSS Information Security Office

Date: January 16, 2007

Version: 1.0

Department of Child Support Services

INFORMATION SECURITY MANUAL	NUMBER:	2000
Subject: Asset Protection Policy	**REVISED DATE:**	**09/24/2009**

Section 1: Introduction

The Department of Child Support Services (DCSS) has the responsibility of maintaining the confidentiality, integrity, and availability of Child Support Information for all California Child Support Program stakeholders. To achieve this goal, it is essential that Applicable Organizations' Management effectively manage Child Support Information and IT Assets. This Asset Protection Policy contains the following Policy Directives:

- Asset Management Requirements
- Asset Identification and Classification Requirements

Section 2: Roles and Responsibilities

1. DCSS Management will establish a periodic reporting requirement for the DCSS CISO to measure the compliance and effectiveness of DCSS ISM policies and standards.
2. Applicable Organizations' Management will be responsible for implementing the requirements of DCSS ISM within their respective organizations.
3. Applicable Organizations' Management, in cooperation with the DCSS CISO, is required to train employees on DCSS ISM policies and standards.
4. Child Support Employees will comply with DCSS ISM policies and standards.

Section 3: Policy Directives

3.1 Asset Management Requirements

Asset Management lays the foundation for the DCSS Asset Protection Program and establishes the management framework for asset identification, classification, access management and security architecture procedures. The following requirements are to be applied at the DCSS and by all Applicable Organization.

3.1.1 DCSS CISO Requirements

1. DCSS CISO, in cooperation from Applicable Organizations' Management, will implement a Risk Management Program to appropriately address risks associated with Child Support Information and Child Support IT Assets.
2. DCSS CISO, in cooperation from Applicable Organizations' Management, is responsible for developing and maintaining inventory of systems that process and store Child Support Information.
3. DCSS CISO will develop and maintain procedures to ensure that Child Support Information and Child Support IT Assets are classified pursuant to ISM 2103 Information and IT Asset Classification Standard.

3.1.2 DCSS Management Requirements:

DCSS Managers will:

1. Use a formal review cycle for all Asset Management activities. At a minimum, the review cycle will include evaluation, and revision if necessary, of asset classification and identification methods.
2. Assign asset owners and/or asset custodians to all DCSS owned and/or managed assets and hold the assigned persons responsible for ensuring that confidentiality, integrity and availability requirements are met.
3. Establish standards for asset life cycle management from acquisition to disposition.
4. Develop metrics for establishing potential impact on DCSS should there be a breach of security and a loss of confidentiality, integrity, or availability of Child Support Information or Child Support IT Assets.
5. Use these metrics to establish the need for appropriate controls and/or technologies that protect Child Support Information or Child Support IT Assets based on their value, confidentiality, and sensitivity.

3.1.3 Applicable Organizations' Requirements

Applicable Organizations' Management will:

1. Support the ongoing development and maintenance of the DCSS Asset Protection Program.
2. Commit to the ongoing training and education of staff responsible for the administration and/or maintenance of Child Support IT Assets and staff with access to Child Support Information.
3. Establish Business Continuity and Contingency Plans in order to assure the accessibility and availability of assets critical to its effective child support operations.
4. Utilize change management and release management processes to ensure only authorized updates and changes are made to all Child Support IT Assets.
5. Establish procedures for approval of the handling of Child Support Information or Child Support IT Assets based on their access, classification and identification requirements.
6. Report to the DCSS CISO, any misuse of Child Support Information or Child Support IT Assets, pursuant to ISM 3100 Security Incident Management Standard.

3.1.4 Asset Owners' and Asset Custodians' Requirements

Asset Owners and Asset Custodians will be responsible for implementing access control authorization for all Child Support Information and Child Support IT Assets. The DCSS Access Control Process will provide standards for identification and authorization of all Child Support IT Asset users.

3.1.5 Child Support Employees

Child Support Employees will:

1. Adhere to DCSS Security Policies, Standards and Procedures.

2. Attend security awareness training annually.

3.2 Asset Identification and Classification Requirements

Applicable Organizations' Management is responsible for protecting Child Support facilities, Child Support Information and Child Support IT Assets. The following requirements address how Applicable Organizations will meet their responsibilities.

1. All Child Support IT Assets must have an owner. Asset owners (Owner) are managers of organizational units that have primary responsibility for information assets associated with their functional authority as defined in State Administrative Manual Section 5320, Asset Protection.
2. Each Child Support IT Asset must have a clearly defined custodian. An asset custodian (Custodian) is a person who, while not necessarily the asset owner, has the responsibility for the proper handling and safekeeping of assets in their custody. Each asset custodian must properly protect Child Support IT Assets in keeping with the designated Owner's control, data sensitivity and data criticality instructions.
3. Systems (including hardware, software and network) that process or access Child Support Information must be inventoried.
4. All users of Child Support IT Assets must be identified as individuals, groups, organizations or processes and the appropriate access policy for each identified entity must be applied for accessing any DCSS asset.
5. Child Support IT Assets and Child Support Information must be classified to ensure compliance with applicable laws, regulations, contractual, and administrative requirements using the classification scheme in ISM 2103 Information and IT Asset Classification Standard. When information of various classifications is combined, the resulting collection of information or new information must be classified at the highest level of control among all the sources.
6. DCSS Management as well as the assigned asset owner and/or custodian must review and approve all reclassification of assets, especially the reclassification of assets to a less sensitive category.
7. The DCSS CISO will ensure that any contract with external third-party organizations that require the exchange of Child Support Information other than that classified as Public will contain definitions of data classifications and the conditions of use of the Child Support Information prior to the exchange of confidential or personal Child Support Information.

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: References

SAM Chapter 5320 - Asset Protection

Section 6: Control and Maintenance

Date Issued: January 16, 2007

Owner: DCSS Information Security Office

Version: 2.0

Department of Child Support Services

INFORMATION SECURITY MANUAL	NUMBER:	2100
Subject: Access Control Standard	**EFFECTIVE:**	**01/16/2007**

Section 1: Introduction

Access controls are measures for ensuring that only users with the proper need and authority can access the system and perform authorized functions on the systems containing child support information.

Applicable Organizations' Management and staff will understand their responsibilities relative to access control. This access control standard contains the following directives:

- Access Control Rules
- Requirements for Access Control
- User Access Management
- Application Access Control
- Monitoring-System Access and Use

Section 2: Standard Directives

2.1 Access Control Rules

Access to Child Support Information and IT assets will be managed using two complementary security principles: "the need to know" and "the least privilege."

1. Access control should start by denying access to everything, and then explicitly granting access according to the "need to know" principle. Child Support Employees should be granted access to Child Support Information or Child Support IT Assets necessary to carry out Child Support Program responsibilities.
2. Access to Child Support Information and Child Support IT Assets should be based on the principle of "least privilege," that is, grant no user greater access privileges to the information or assets than Child Support Program responsibilities demand.
3. The "least privilege" principle should also be applied to users' modes of access, such as whether the individual is granted "read or write" privileges.

2.2 Requirements for Access Control

These access control requirements apply to any system that processes or stores Child Support Information and Child Support IT Assets.

2.2.1 Documentation and Process Requirements

1. Child Support Information and IT Assets Owners will determine the classification of Child Support Information and Child Support IT Assets which they own, and will document access requirements applicable to that information or asset.

2. Applicable Organizations' Management will:
   a. Develop access control standards that clearly define the needs of each user or group to access Child Support Information and Child Support IT Assets using the need to know and the least privilege principles.
   b. Establish user profiles detailing privileges and access rights for each profile to facilitate assignment of access to each user.
   c. Develop and maintain procedures or system controls to ensure that:
      i. Access to Child Support Information and Child Support IT Assets is systematically controlled, i.e. granting, changing and deleting access privileges to information-systems.
      ii. Account deletion or disablement notifications are communicated to the designated administrators in a timely manner.
      iii. User and group file-access rights are configured according to business requirements and the Applicable Organizations' access control standards.
      iv. Accounts for employees who take extended leaves of absence (30 days or longer) are disabled.
      v. Audit processes are performed to identify and report inactive accounts.
      vi. Delegation and maintenance of the password system is limited to a select number of people.
      vii. Have procedures in place to quickly notify those responsible to modify or disable access when there are personnel changes.[1]
3. All individuals with access to Child Support Information and Child Support IT Assets will attend security awareness training and sign confidentiality statements consistent with ISM 6000 Security Awareness Policy.

2.2.2 System Requirements

Any system that processes or stores Child Support Information will:

1. Meet the ISM 2101 Password Standard.
2. Strictly control access enabling only privileged users or supervisors to override system controls or the capability of bypassing data validation on editing problems. [2]
3. Monitor special privilege access, e.g. administration accounts.
4. Restrict authority to change master files to persons independent of the data processing function.[3]
5. Have access control mechanisms to prevent unauthorized access or changes to data, especially, the server file systems that are connected to the Internet, even behind a firewall.
6. Be capable of routinely monitoring the access to automated systems containing Child Support Information. [4]
7. Log all modifications to the system files.[5]

---

[1] Automated Systems for Child Support Enforcement: A Guide for States, August 2007, Requirement H-2f

[2] Ibid, requirement H-4b

[3] Ibid, requirement H-4a

[4] Ibid, requirement H-2k

8. Limit access to system utility programs to necessary individuals with specific designation.[6]
9. Maintain audit logs on a device separate from the system being monitored.
10. Delete or disable all default accounts.
11. Restrict access to server file-system controls to ensure that all changes such as direct write, write access to system areas and software or service changes will be applied only through the appropriate change control process.
12. Restrict access to server-file-system controls that allow access to other users' files.
13. Ensure that servers containing user credentials will be physically protected, hardened and monitored to prevent inappropriate use.

2.2.3 Logon Banners and Warning Notices

1. All computer systems that contain or access Child Support information will display warning banners informing potential users of conditions of use consistent with state and federal laws.
2. Warning banners must remain on the screen until the user takes explicit actions to log on to the information system.
3. The banner message will be placed at the user authentication point for every computer system that contains or accesses Child Support Information. The banner message may be placed on an initial logon screen in situations where the logon provides access to multiple computer systems.
4. At a minimum, banner messages must provide appropriate privacy and security information and shall contain information informing potential users that:
    - User is accessing a Government information system for conditions of use consistent with state and federal information security and privacy protection laws.
    - System usage may be monitored, recorded, and subject to audit.
    - Unauthorized use of the system is prohibited and subject to criminal and civil penalties.
    - Use of the system indicates consent to monitoring and recording.

2.3 User Access Management

This section describes the user access lifecycle from granting user access to termination of access:

2.3.1 User Identification and Authentication

Access control is the process of limiting and controlling access to system resources, and user identification (ID) and authentication is the most fundamental aspect to control access.

Applicable Organizations' Management will ensure that systems that contain or store Child Support information:

1. Uniquely identify each individual user.
2. Authenticate user identities at logon. Authentication mechanisms will be appropriate to the sensitivity of the information.

---

[5] Ibid, requirement H-2j

[6] Ibid, requirement H-3g

3. Provide accountability for each user's activity using Child Support Information.

2.3.2 User Registration

User registration is a process that documents access levels authorized for each Child Support Employee, ensures user identity and the need to access Child Support Information and Child Support IT Assets. Applicable Organizations' Management will establish and maintain user registration procedures that apply to all stages of user access life cycle, from registration of new users to de-registration of users no longer authorized to have access. The user registration procedures will:

1. Track or document which individuals are authorized to issue user IDs to Child Support Employees and restrict authority to issue user IDs to those identified individuals.
2. Track or document the access control level privileges that may be granted and restrict individuals' access to authorized levels.
3. Track or document the access levels granted to each registered Child Support Employee.
4. Conduct regular reviews of the registered Child Support Employees' access level privileges.
5. Provide procedures to disable user accounts upon termination of employment or contractual obligation, and procedures to modify access privileges upon change in job responsibilities.
6. Secure password delivery and password reset mechanisms to assure passwords are known only to the user.

2.3.3 Account and Access Management

The following account and access management processes applies to all Applicable Organizations:

1. Child Support Employees should be assigned only the access privileges needed for their job.
2. For any system that processes or stores Child Support Information, password security will extend to the functional screen level and limit the user's capability to view and/or update those screens. [7]
3. System administration accounts should be assigned and used only for performing administrative activities. For example, do not log-in with administrative account when using the system as a regular user, not performing administrative duties.
4. Each user will have a unique user-id. Accounts should NOT be shared at anytime.
5. Child Support Employees should log off or activate password-protected mechanisms (e.g., password-protected screensavers) before leaving the immediate vicinity of Child Support Systems whenever possible.

2.3.4 Inactivity Timeout and Restricted Connection Times

Systems that process or store Child Support Information shall implement the following:

1. Automatic lockouts for system devices, including workstations or other mobile computing devices, after no more than 10 minutes of inactivity. Refer to ISM 2104 for mobile computing devices.

[7] Ibid, requirement H-2c

2. Automatic network session termination for network connections associated with a communications session at the end of a session after no more than 10 minutes of inactivity.[8]

2.4 Application Access Control

For any system that processes or stores Child Support Information, controls should be used to restrict access within application systems. Logical access to software and information should be limited to authorized users only. Application system controls should:

1. Control user access to information and application system functions, according to a defined access-control policy.
2. Prevent unauthorized access to any utility or operating-system software that can override system or application controls.
3. Prevent compromise to the security of other systems with which information resources are shared.
4. Allow access only to the owner of information and other authorized users or groups.
5. Carefully manage all interfaces.
6. The system will provide security levels for access to records and files.[9]

2.5 Monitoring-System Access and Use

See ISM 2105 Secure System Standard, for system monitoring requirements.

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 2000 – Asset Protection Policy

ISM 2101 – Password Standard

---

[8] NIST SP 800-53 SC-10; IRS P1075 5.6.15

[9] Ibid, requirement H-2e

ISM 2102 – Remote Access Standard

ISM 2103 – Information and IT Asset Classification Standard

Section 5: References

SAM 5340 – Access Control

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

Section 6: Control and Maintenance

Owner: DCSS Information Security Office

Revised: May 1, 2010

Department of Child Support Services

INFORMATION SECURITY MANUAL	NUMBER:	2101
Subject: Password Standard	**EFFECTIVE:**	**01/16/2007**

Section 1: Introduction

Passwords are the first line of protection for user accounts. Poorly managed passwords could become the weakest security link and may result in the compromise of Child Support Information and IT Assets. These standards establish the minimum requirements to create and to maintain a secure environment.

This Password standard contains the following directives:

- Password Requirements enforced by systems
- Password rules for users

Section 2: Standard Directives

2.1 Password Requirements Enforced by Systems

These password requirements apply to all systems processing or storing Child Support Information:

1. Passwords must contain at least 8 characters unless the system incapable of compliance with this requirement. For systems that cannot accept a password of 8 characters, the minimum password length will be the maximum length accepted by that system.
2. The system must automatically require the system user to periodically change passwords.[1] Passwords will be changed every 60 days. For systems which cannot accept a password length of 8 characters or cannot meet the complexity rule, the password will be changed every 45 days.
3. Passwords must satisfy the complexity rule i.e. the password must contain at least 3 of the following 4 elements: uppercase and lowercase letters, Numeric, and punctuation or special characters such as a, @, #, $, %.
4. Passwords must not be reused for six iterations.
5. Audit logging will be enabled to detect invalid log-in attempts.
6. The user account must be automatically disabled after three unsuccessful logon attempts. Users can regain access only through reset methods authorized by the Applicable Organization's Management.
7. After a user password reset, the system must require the user to change password at the first logon attempt following the reset.
8. Passwords files must be encrypted using one way hashing algorithms to prevent

[1] ACF Requirement H-2c

compromise and disclosure when stored in files or databases on systems and servers. Microsoft's LM and NTLM hash must not be used to store passwords as these files are easily compromised. If passwords cannot be encrypted, access to the file or database element containing the passwords must be restricted to authorized system administrators.

9. Default passwords must be changed before the device is placed in service.

2.2 Password rules for users

Users must:

1. Use a password no less than 8 characters unless the system cannot support a password of specified length.
2. Not reveal their passwords to anyone, at anytime, for any reason.
3. Not store their passwords in an unencrypted format for reference.
4. Change their password if a compromise is suspected.
5. Select complex passwords—that is passwords that combine 3 of the following 4 elements: uppercase and lowercase letters, numeric digits, and punctuations and special characters such as @, #, $, .,%, ^, &.
6. Not use sequential or repeating combinations, such as "12345678," "222222," "abcdefg," or adjacent letters on the keyboard.
7. Consider using a pass phrase if the system can accept lengthy passwords. A passphrase is a sequence of words or other text. Examples of such phrases appear below:
   a. The sky is 2 Bright! (complexity = upper and lower case, a numeric character and a special character)
   b. 1 Sleek silveR cruiser gulps gas. (complexity = numeric, upper and lower case and a special character)
   c. Who 8 the chocolate cake? (Complexity = upper and lower case letters, numeric digit and special character).
8. Consider using a pass phrase mnemonic. A pass phrase mnemonic uses the first or representative characters of each word in the pass phrase and converts the pass phrase into a word that meets the complexity rules. Examples of such phrases appear below:
   a. pass phrase = I wish there was a Lexus in my driveway! Pass phrase mnemonic = IwtwaLimd! (Complexity = upper and lower case and a special character.
   b. Pass phrase = I am 56, too old to keep working this hard every day. Pass phrase mnemonic = Ia56,totkwthed! (Complexity = upper and lower case, numeric and special character).
9. Not use single common or dictionary word with letters replaced by numbers or symbols, such as "M1cr0$0ft" or "P@ssw0rd".
10. Not use the "Remember Password" feature of applications.
11. Not write down passwords unless properly secured. In the case of storing password(s) in an electronic data file, the file must be encrypted.
12. Not include the username or User ID and password in the same e-mail or other form of communication when distributing account information. User ID and password should be sent

in separate email messages or two separate modes of communication.

13. Not use a password that can be easily guessed such as the user's user-id, name, or nicknames.
14. Use a unique password for each account that has system-level privileges granted through group memberships or programs such as "sudo".
15. Change the passwords of all accounts to prevent subsequent use when the holder of one of these accounts leaves.
16. Not use child support system passwords for accessing personal resources (e.g., personal bank accounts, web stores, etc.).

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 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 2000 – Asset Protection Policy

ISM 2100 – Access Control Standard

Section 5: References

State Administrative Manual Section 5335.1 – Information Integrity and Data Security

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

Section 6: Control and Maintenance

Owner: DCSS Information Security Office

Revised: May 1, 2010

Department of Child Support Services

INFORMATION SECURITY MANUAL	NUMBER:	2102
Subject: Remote Access Standard	**REVISED DATE:**	**09/24/2009**

Section 1: Introduction

For the purpose of this standard, Remote Access is defined as the ability to access Child Support Information or IT Assets of an Applicable Organization from a device that is outside of the organization's network.

While some child support functions must be conducted from remote locations, unauthorized and unmanaged Remote Access may expose Child Support Information and IT Assets to risks and vulnerabilities. Accordingly, Remote Access to Child Support Information and IT Assets must be provided only to individuals with a verified business need for such access and only under conditions that protect the confidentiality, integrity, and availability of the information and IT assets. The Remote Access Standard directives are described in the following sections:

- Remote Access Authorization
- Remote Access System Requirements
- Remote System Configuration Requirements
- Remote Access User Requirements
- Documentation

Section 2: Standard Directives

2.1 Remote Access Authorization

1. Applicable Organizations must develop a Remote Access authorization process to ensure Remote Access to Child Support Information and IT Assets is granted based on business needs. This process must include a "Remote Access Request Form" that requires the user to detail the access needed, describe the business need, and certify knowledge and acceptance of this standard. The form must also detail acceptable use policies and consequences of unauthorized access or disclosure.
2. The Remote Access solution must leverage end to end encryption such as Virtual Private Network (VPN) or Secure Socket Link (SSL).
3. The Remote Access solution must ensure that the user credentials are exchanged in an encrypted format.
4. Applicable Organizations must monitor Remote Access to ensure compliance with requirements and appropriate use.
5. Remote Access must only be allowed from devices owned, managed, and controlled by the Applicable Organization with the following exception:
    a. Personally owned or non Applicable Organization owned devices may be used only to access Web Based applications (such as email and calendar services) containing information classified as Sensitive or Public.

Note: Information classified as Personal or Confidential may NOT be accessed using personally owned or non Applicable Organization owned devices (i.e. devices owned by court facilities, public libraries, airports, or privately owned businesses).

2.2 Remote Access System Requirements

1. All Remote Access must be authenticated with a minimum of a unique login name and a unique password unless strong authentication[1] is used. Strong authentication is highly recommended for Remote Access to Child Support Information or IT Assets classified as confidential, personal, or sensitive.
2. If applicable, Remote Access users and equipment must comply with ISM 2104 Mobile Computing Device Standard.
3. Remote Access equipment must comply with ISM 2111 Encryption Standard.
4. Remote Access using wireless connections must comply with ISM 2114 Wireless Communication Standard.

2.3 Remote Access Configuration Requirements

Equipment used for Remote Access to Child Support Information and Child Support IT Assets must be configured securely according to the following:

1. Screen saver must automatically activate after 10 minutes and require a password.
2. Antivirus software must be installed, enabled for “real-time” scans, enabled for automatic anti-virus definition updates.
3. “Critical” or “Security” software patches must be installed to ensure that software is kept current.
4. Systems must only contain software authorized by DCSS or the Applicable Organization.
5. All unnecessary services and ports must be disabled.
6. Only enable TCP/IP protocol.
7. Unnecessary ports on the personal firewall must be disabled or blocked.
8. File sharing and/or peer-to-peer programs are strictly prohibited.
9. Apply security best practices as recommended by the National Institute of Standards and Technology (NIST).

[1] Strong authentication is defined as the combination of at least two authentication components from the following areas: something you know (a login name, a password), something you have (token, card key), or something you are (voiceprint, fingerprint, retinal scan).

2.4 Remote Access User Requirements

Remote access users must:

1. Obtain management approval prior to using Remote Access services.
2. Have a legitimate business need for Remote Access to Child Support Information or IT Assets.
3. Use Remote Access services only for child support business.
4. Agree to the requirements detailed in this standard by signing the Remote Access Request Form.

2.5 Documentation

All Applicable Organizations that authorize Remote Access to Child Support Information and IT Assets will implement a process to manage Remote Access. The process will include:

1. Procedures to verify that only users with a legitimate business need are authorized for Remote Access.
2. Procedures to verify that Remote Access is removed or disabled when the user no longer requires Remote Access.
3. Procedures to ensure that Remote Access Request Forms are retained and made available to DCSS upon request.
4. A tracking system to monitor Remote Access.
5. Audit procedures to ensure adherence to the above standards.

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 2000 – Asset Protection Policy

ISM 2100 – Access Control Standard

ISM 2101 – Password Standard

ISM 2104 – Mobile Computing Device Standard
ISM 2111 – Encryption Standard
ISM 2114 – Wireless Remote Communication Standard

Section 5: References

SAM Section 5335 – Communications and Operations Management
NIST SP 800-63 – Electronic Authentication Guideline

Section 6: Control and Maintenance

Date Issued: January 16, 2007
Owner: DCSS Information Security Office
Version: 2.0

Department of Child Support Services

INFORMATION SECURITY MANUAL	NUMBER:	2103
Subject: Information and IT Asset Classification Standard	**REVISED DATE:**	**09/24/2009**

Section 1: Introduction

Child Support Information an IT Asset Classification is required to ensure appropriate protection methods are adopted to protect the confidentiality, integrity, and availability of Child Support Information and Child Support IT Assets.

Section 2: Standard

Pursuant to State Administrative Manual Section 5320.5, Child Support Information is classified as: Public, Personal, Confidential and Sensitive. Each classification description includes a definition, and an example to assist the data owner in identifying the proper classification.

2.1 Confidential

Definition: Information that is protected by law from unauthorized access and disclosure and that has value to the public that is jeopardized unless access is restricted to specific individuals or business functions.

Examples:

1. Child Support Participant application for Child Support Program services.
2. Preliminary drafts, notes, or interagency or intra-agency memoranda that are not retained by the public agency in the ordinary course of business.
3. Records pertaining to pending litigation or claim.
4. Medical or similar files, the disclosure of which would constitute an unwarranted invasion of personal privacy.
5. Test questions, scoring keys, and other examination data used to administer a licensing examination or examination for employment.
6. Documents protected by attorney-client privilege.
7. Correspondence of and to the Governor or employees of the Governor's office or in the custody of or maintained by the Governor's Legal Affairs Secretary.
8. Home addresses and home telephone numbers of state employees.
9. System and network information, such as diagrams, IP addresses, etc.
10. Employment Data.
11. Federal Tax Information.

2.2 Personal

Definition: Information that is protected by law from unauthorized access and disclosure, the disclosure of which requires the owner of the data to notify the impacted individual(s). Notice-triggering personal information means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:

- Social security number.
- Driver's license number or California Identification Card number.
- Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.
- Medical information (as defined in Civil Code Sections 1798.29).
- Health information (as defined in Civil Code Section 1798.29).

(See Civil Code Sections 1798-29.)

Examples:

1. Child support records containing participant's name and social security number.
2. Child Support Participant bank account number and access code.
3. Employee personnel records that contain employee's name and California driver's license number or Social Security Number.
4. Family Violence participant data.

2.3 Sensitive

Definition: Data essential to the on-going operation of Applicable Organizations. It allows the organization to conduct its internal business and maintain support of its applications and business processes. Protection mechanisms are typically focused on the sensitivity of disclosure outside of a business function. Additionally, the availability of the data must support the criticalness of the business function.

Examples: Information on Intranets, internal memoranda, strategic plans, recruitment plans, budgets, phone lists, policies and standards.

2.4 Public

Definition: Any information prepared, owned, used, or retained by a state agency and not specifically exempt from the disclosure requirements of the California Public Records Act (Government Code Sections 6250-6265) or other applicable state or federal laws. Public data is suitable for public dissemination and can be easily reproduced from other sources. Protection mechanisms are typically focused on integrity and availability.

Example: Public Internet content, service availability, mission statements, domain name services, outreach materials, procurement announcements, Feasibility Study Reports, etc.

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 2000 – Asset Protection Policy

Section 5: References

State Administrative Manual Section 5320.5 Classification of Information

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

California Family Code Section 17212

California Civil Code Section 1798

Section 6: Control and Maintenance

Owner: DCSS Information Security Office

Date Issued: January 16, 2007

Version: 2.0

Department of Child Support Services

INFORMATION SECURITY MANUAL	NUMBER:	2104
Subject: Mobile Computing Device Standard	**EFFECTIVE:**	**01/16/2007**

Section 1: Introduction

A Mobile Computing Device (MCD) is a device that may be used to access Child Support Information, Applicable Organizations' networks, or to send and receive messages while a user is away from his or her desk. MCDs include but are not limited to: Laptops, Personal Digital Assistants (PDA), Blackberries, Smart Phones and Text Pagers. While MCDs offer Child Support Employees a valuable tool to conduct Child Support business, they also pose several security risks in regards to keeping Child Support Information secure from unauthorized access. Such devices also present risks of introducing threats into Applicable Organizations' networks and Child Support IT assets. Any device that is designed to be mobile and has the capabilities to access Child Support Information or send and receive confidential and/or sensitive personal information is bound by this standard.

Section 2: Standard Directives

2.1 MCD Applicable Organizations' Requirements

To ensure that MCDs do not introduce threats into systems that process or store Child Support Information, Applicable Organizations' Management will:

1. Establish and manage a process for authorizing, issuing and tracking the use of MCDs.
2. Permit only authorized MCDs to connect to Child Support IT Assets or networks that store, process or connects to Child Support Information IT Assets.
3. Enforce authentication using a password at a minimum.
4. Implement applicable access control requirements in accordance with ISM 2100 Access Control, such as the enforcement of a system or device lockout after 10 minutes of inactivity requiring reentering of a password to unlock.
5. Install an encryption algorithm that meets or exceeds industry recommended encryption standard for any MCD that will be used to store Child Support Information. See ISM 2111 Encryption.
6. Ensure that MCDs are configured to restrict the user from circumventing the authentication process.
7. Provide security awareness training to Child Support Employees that informs MCD users regarding MCD restrictions.
8. Recommend that users label MCDs with an address or phone number so that the device can be returned to the owner if recovered.

2.2 MCD User Requirements

Child Support Employees that utilize authorized MCDs to connect to Child Support IT Assets or networks will take precautions to prevent theft, loss, damage and/or unauthorized viewing of data stored on their MCD. Accordingly, Child Support Employees will:

1. Not leave an MCD device unattended in a public place.
2. Not allow an unauthorized person to use or view the data contained on it.
3. Not use an MCD to synchronize the user's personal computer or other equipment that has not been issued and configured by the Applicable Organization.
4. Report any lost or stolen MCD in accordance with ISM 3100 Security Incident Management Standard.

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 2000 – Asset Protection Policy

ISM 2111 – Encryption

Section 5: References

State Administrative Manual Section 5335.2 – Personal Computer Security

Section 6: Control and Maintenance

Owner: DCSS Information Security Office

Revised: May 1, 2010

Department of Child Support Services

INFORMATION SECURITY MANUAL	NUMBER:	2105
Subject: Secure System Standard	**EFFECTIVE:**	**01/16/2007**

Section 1: Introduction

For the purpose of this standard, a system is defined as any Child Support IT Asset that is used for processing and storing Child Support Information including but not limited to software, hardware, and business applications. All Applicable Organizations must demonstrate that the incorporation of effective security measures is an integral part of the system development process and/or the system management processes used by the organization.

This standard contains the following directives:

- System Controls
- Audit Tracking Requirements
- Test Environment

Section 2: Standard Directives

2.1 System Controls

The following Federally required controls must be included in all systems that store or process Child Support Information:

1. Override capability, or bypassing of data validation on editing problems, must be restricted to supervisory personnel.[1]
2. System development must include recovery and re-start capabilities for events such as operator errors, data errors and/or hardware/software failures.[2]
3. The system must generate record counts to validate the completeness of data processed.[3]
4. All rejected data must [4]be automatically written to a suspense file and including a record count.
5. Separation of general (e.g., non-privileged) user functionality from administrative-management (e.g., privileged) user functionality.[5] The information system shall prevent the presentation of management-related functionality at an interface for general users, whenever possible.
6. System design to prevent unauthorized or unintended information transfer via shared system resources.[6]

---

[1] Automated Systems for Child Support Enforcement: A Guide for States, August 2007, requirement H-4b

[2] Ibid, requirement H-3c

[3] Ibid, requirement H-4d

[4] Ibid, requirement H-4e

[5] NIST SP 800-53 SC-2

[6] NIST SP 800-53 SC-3

2.2 Audit Tracking Requirements

In accordance with Federal Child Support regulations all systems that store or process Child Support services must be compliant with the following audit tracking requirements:

1. The system must be capable of maintaining information on all changes to critical records and/or data fields (e.g., Arrearage Balances, Monthly Court-Ordered Support Amounts, SSN, Name, Family Violence Indicator, etc.) including identification of the responsible system user/caseworker and date/time of the change.[7]
2. The system must provide complete and accurate internal audit trails of all financial management activities, e.g. billing, receipting and distribution, and support order changes. [8]
3. The system must detect, record, and lock out unauthorized attempts to gain access to system software and data. [9]
4. The system must be capable of routinely monitoring the access to use of the automated system. [10]
5. An audit trail of all operating system actions must be maintained either on the automatic console log or on the computer system's job accounting file.[11]
6. Audit logging should include capabilities for the following:
    a. Capture successful logon and logoff attempts.
    b. Capture unsuccessful login and authorization attempts.
    c. Capture what users get access to what information and with what permissions, including read-only or view access.
    d. Identify a specific user with responsibility for any transaction.
    e. Identify all activities that involve changes to system configurations and ability to identify which users performed the activity.
    f. Date and time-stamp log entry.
    g. Restrict audit trail to personnel routinely responsible for performing security audit functions.
7. Standard retention of log files is for two (2) years. Retention for log files that track access to federal tax information (FTI) must be archived for six (6) years to enable the recreation of computer-related access. Log file retention periods must be maintained to satisfy the purpose for which it was created, and to fulfill operational, legal, fiscal, administrative, and prudent business requirements. If log files are needed for legal or approved audit purposes beyond the recommended retention period, retention periods may be exceeded without notice. Shorter retention periods should be considered for logs that are prepared for the purpose of selective audits.

Note: Systems that (do not) contain or process Child Support information must review the applicability of each audit tracking requirement and implement appropriate mechanisms to protect information and systems.

---

[7] Ibid, requirement H-2i

[8] Ibid, requirement H-3f

[9] Ibid, requirement H-2g

[10] Ibid, requirement H-2k

[11] Ibid, requirement H-3e

2.3 Test Environments

Applicable Organizations must comply with the following requirements:

1. Test environments should be physically and logically separate from, but closely replicate the production environment.
2. All testing of programs must be accomplished using test data in a test environment, as opposed to live (production) data.[12] Using copies of production data in a test environment is acceptable when necessary to adequately test the system.

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 2000 – Asset Protection Policy

Section 5: References

SAM Section 5345 – Information Systems Acquisition, Development and Maintenance

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

Section 6: Control and Maintenance

Owner: DCSS Information Security Office

Revised: May 1, 2010

[12] Ibid, requirement H-3d

Department of Child Support Services

INFORMATION SECURITY MANUAL	NUMBER:	2107
SUBJECT: CONFLICT RECUSAL STANDARD	EFFECTIVE:	01/16/2007

Section 1: Introduction

Child Support Employees must conduct their daily child support business with the utmost integrity. Child Support Employees must avoid impropriety in conducting their business. Accordingly, Child Support Employees must recuse themselves from cases in which one participant is:

1. The Child Support Employee
2. A relative of the Child Support Employee
3. A person with whom the Child Support Employee cohabits
4. A person with whom the Child Support Employee has Personal or Business Relationship

Section 2: Standard Directives

2.1 Definitions

Conflict Recusal	A commitment from a Child Support Employee that because he or she has a personal relationship with an individual in a child support case he or she relinquishes access to any Child Support Information about that case.
Relative	Individuals that are related by blood, marriage or adoption including the following relationships: spouse, child, stepchild, parent, stepparent, grandparent, grandchild, brother, sister, half-brother, half-sister, aunt, uncle, niece, nephew, parent-in law, daughter-in-law, son-in-law, brother-in-law, sister-in-law, and first cousin.
Cohabit	The act of sharing a residence with another individual regardless of whether or not the persons sharing the residence have a romantic relationship.
Personal or Business Relationship	An individual with whom the Child Support Employee's relationship can be described as more than a casual acquaintance. The term may include, but not limited to: persons the Child Support Employee is having a romantic relationship with or dating, persons with whom the Child Support Employee regularly spends time, and persons that regularly provide day care to the Child Support Employee's child(ren).

2.2 Employment and Procurement Notices

Applicable Organizations' Management will include in procurement documents and employment opportunity announcements, a statement informing potential vendors and job candidates that upon selection or hire individuals that are provided access to Child Support Information must recuse themselves from cases in which one participant is:

1. The Child Support Employee.
2. A relative of the Child Support Employee.

3. A person with whom the Child Support Employee cohabits.
4. A person with whom the Child Support Employee has Personal or Business Relationship.

Section 3: Employee Conflict Recusal Requirements

1. Applicable Organizations' Management will implement procedures necessary to ensure that Child Support Employees recuse themselves pursuant to this standard. Such procedures will include:
   - Instructions for Child Support Employees for requesting case recusal.
   - The steps for system administrators to restrict access to cases in systems containing Child Support Information in which the Child Support Employee has recused himself or herself.
   - Procedures to search system data bases for every Child Support Employee to determine if he or she has failed to declare his or her own child support case.
2. Child Support Employees will not access any form of Child Support Information regarding any case in which he or she has a relationship as specified in this standard with any of the case's participants.
3. Child Support Employees will recuse themselves from appropriate cases pursuant to this standard at the time of hire and at any time that the employee learns that he or she has a relationship, specified in this standard, with a child support participant in any case.
4. Applicable Organizations' Management will develop procedures to make the employees and personnel with access to Child Support Information aware of this standard, the recusal responsibility and the procedures to submit recusal.

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 Standard

Section 6: References

SAM Section 5320.2 – Responsibilities of Owners of Information

Section 7: Control and Maintenance

Owner: DCSS Information Security Office
Revised: September 24, 2009
Version: 2.0

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

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

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.

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

Owner: DCSS Information Security Office

Date Issued: September 24, 2009

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

Owner: DCSS Information Security Office

Date Issued: September 24, 2009

Version: 1.0

Department of Child Support Services

INFORMATION SECURITY MANUAL		NUMBER: 2110
Document Type:	Standard	**EFFECTIVE:** 05-01-10
Subject:	Media Protection and Sanitation	
Synopsis:	Establishes protection requirements for handling paper and digital storage media, including sanitization.	

Section 1: Introduction

Media protection controls provide physical and environmental protection and accountability of Child Support Information on storage media of all types (such as magnetic, optical, solid state and paper) regardless of its form, whether digital or non-digital (paper). For the purpose of this standard, media is defined as any storage component that contains or stores Child Support Information, such as but not limited to printouts and hard copy documents, tapes, diskettes, flash memory drives (USB, jump, thumb), hard drives, CDs, DVDs, etc. Media may be found in devices, such as PDAs, desktops, laptops, servers, and other digital devices. Media protection controls should be designed to prevent the loss of confidentiality, integrity, or availability of information. This standard establishes physical, logical, and environmental protection requirements for media.

Standard directives include the following:

- Media Access and Storage
- Media Sanitation

Section 2: Standard Directives

2.1 Media Access and Storage

Applicable Organizations shall establish procedures and take the following actions to ensure that media is protected from unauthorized access, disclosure, modification, destruction or loss.

1. Restrict access to all media to authorized individuals with processes and/or mechanisms for authentication and authorization in accordance with ISM 2000 Access Control.
2. Physically control and securely store all media within controlled or normal work areas and protect from physical and environmental hazards. This includes but is not limited to employee desks or other local and remote work areas. Storage areas with significant volumes of media should employ automated mechanisms to restrict and audit access.
3. Maintain confidentiality and acceptable use statements for system users in accordance with ISM 5000 Acceptable Use.
4. Classify media in accordance with ISM 2103, Information and IT Asset Classification, commensurate with the highest level of information processed on the system with which it is used.
5. Mark removable or portable media containing Federal tax returns and/or return information (FTI) as FTI to ensure proper handling and storage.

6. Protect and control media when traveling outside of normal work areas, and restrict the activities associated with the transport of such media to authorized personnel.
7. Employ the use of encryption in accordance with ISM 2111, Encryption when transporting digital media that contain Child Support Information.
8. Remove and/or sanitize digital media, where applicable, prior to sending off-site for maintenance.
9. Document activities associated with the transport of media containing Child Support Information with the use of logs or other tracking mechanisms.
10. Implement use of inventory logs, control numbers or other record-keeping methods in addition to appropriate physical protection for media containing FTI, which requires strict access accountability and/or chain-of-custody verification (including media sent off-site for maintenance). These logs must be archived and made available to the DCSS ISO for six (6) years.
11. Ensure Child Support Information Custodians are advised of security requirements and/or data sharing agreements to establish procedures for compliance with those requirements.
12. Permit only authorized digital media to process, access, and store Child Support Information.
13. Protect any media containing Child Support Information until the media are sanitized in accordance with National Security Agency (NSA) standards (for example, purging or destroying) when no longer needed or required. Refer to the DCSS ISO Media Sanitation Guideline, ISM G-10-01.
14. Restrict reuse of digital media used for backup and/or data storage of Child Support Information only to the Applicable Organizations' data.
15. Require offsite facilities used to store paper documents or digital media comply with DCSS media protection and handling requirements and implement the same security provisions with that of the Applicable Organization's security requirements.

2.2 Media Sanitation

Sanitization refers to the destruction of data on media and/or system(s)/device(s) containing such media, as well as the removal of all labels and markings, such that there is reasonable assurance that the data cannot be recovered or reconstructed. Media sanitization mitigates the risks of unauthorized disclosure of information by ensuring that the information on media being disposed, reused (when applicable), or returned to vendors or manufacturers, cannot be recovered or reconstructed. Applicable Organization shall apply the following directives for media sanitation.

1. Sanitization methods for media containing Child Support Information shall be in accordance with NSA standards (for example, clearing, purging, or destroying). Refer to DCSS ISO Media Sanitation Guideline, ISM G-10-01.
2. Acquisitions for equipment intended for the use of processing or storing Child Support Information that include vendor return options for replacement or repair (such as off-site repair or maintenance) should include provisions within the purchase agreement or documentation to allow destruction of all information and/or media prior to return for replacement or repair.
3. All storage media (magnetic, optical, electrical, or other) subject to vendor return agreements (such as but not limited to lease, warranty, rebate/refund etc.) shall have a

method to appropriately sanitize the media of all residual data, using state- and federally-required methods prior to returning to vendor. Refer to the DCSS ISO Media Sanitation Guideline, ISM G-10-01.

4. All contracts or agreements for vendor-provided services for sanitation or disposal of media containing Child Support Information shall include provisions for a Child Support Employee to witness the media sanitation.
5. Prior to surplus, media that is obsolete or no longer usable shall either be purged or physically destroyed to ensure residual data cannot be recovered or reconstructed. Physical destruction methods include disintegration, incineration, pulverizing, or shredding. Refer to DCSS ISO guidelines for specific examples. Refer to DCSS ISO Media Sanitation Guideline, ISM G-10-01.
6. Sanitization procedures and equipment shall be periodically tested, where applicable, to verify correct performance.
7. Hardcopy documents, such as computer printouts, notes, work papers, etc., must be destroyed using methods such as incineration, mulching, pulping, disintegration, or shredding. Hand-tearing or burying Child Support Information in landfills is an unacceptable method of disposal.
8. Sanitization of digital media or electronic surplus property containing FTI shall be witnessed by an Applicable Organization's employee, documented, and certified in writing. Certification records shall include information to identify media that was sanitized/destroyed, such as, property tag numbers, serial numbers and manufacturer, date of sanitization, sanitization method (clear, purge, destroy) and final disposition (vendor return, resale, donation, etc). Certification records for media containing FTI must be retained and made available to the DCSS ISO for six (6) years.

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 ISO 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 ISO 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 2103 – Information and IT Asset Classification Standard

ISM 2108 – Physical Security Standard

ISM 2111 – Encryption Standard

Section 5: References

SAM Section 5320 – Asset Protection

SAM Section 5345.2 – Cryptography

ISO/IEC 27002:2005, Section 10.7 – Media Handling

P1075, IRS Safeguards for Protection Federal Tax Returns and Return Information – Sections 3.2 Electronic Files; 3.3 Non-Electronic Files; 4.5 Handling and Transporting Federal Tax Information; 4.6 Physical Security of Computers, Electronic, and Removable Media; 4.7.1 Equipment; 5.3 Commingling; 5.5 Control over Processing; 5.6.10 Media Access Protection; 5.6.16 System and Information Integrity; 6.3.2 Secure Storage; 7.2.4 System Records; 7.2.7 Disposal; 8.3 Destruction Methods; and 8.4 Disposing FTI-Other Precautions

NIST SP 800-88 – Guidelines for Media Sanitization

Section 6: Control and Maintenance

Issued: May 1, 2010

Owner: DCSS Information Security Office

Department of Child Support Services

INFORMATION SECURITY MANUAL	NUMBER:	2111
Subject: Encryption Standard	**REVISED DATE:**	**09/24/2009**

Section 1: Introduction

The California Child Support Program collects, stores, and processes personal and confidential information to fulfill its mission for the delivery of quality child support establishment, collection, and distribution services. Pursuant to State Administrative Manual (SAM) Section 5335.2, and California Civil Code 1798.29, DCSS is required to protect this information in electronic form from unauthorized access while in storage or in transit by the use of encryption. Encryption is the encoding of data so that it can be read only by the intended recipients or at the intended destination.

Section 2: Standard Directives

2.1 Encryption Requirements

Applicable Organizations must develop procedures to implement the following requirements to protect Child Support Information classified as personal, sensitive, or confidential, per ISM 2103 Information and IT Asset Classification Standard:

1. Encrypt when stored on portable computing devices i.e. Laptops, PDAs, etc.
2. Encrypt when stored on portable storage media i.e. CDs, DVDs, USB flash drives, tapes, removable hard drives, etc.
3. Encrypt when transmitted over a public network. Solutions may include: Secure Socket Layer (SSL), Virtual Private Network (VPN), Secure File Transfer Protocol (SFTP), encrypted email, and/or encrypted wireless networks.
4. Ensure contractors such as business partners or vendors provide the same controls and safeguards to protect sensitive, confidential or personal Child Support Information.
5. When an encryption product is employed, it must be certified according to Federal Information Processing Standards (FIPS Publication 140-2). Use of proprietary encryption algorithms is not allowed for any purpose on Child Support Information or Child Support IT Assets.
6. Encrypt using at a minimum a 128-bit randomly generated key. The encryption algorithm must meet or exceed the current industry standard of Triple DES. However, Applicable Organizations are encouraged to leverage the latest standard approved by the National Institute of Standards and Technology (NIST), such as AES for future implementations.

2.2 Encryption Recommendations

The following encryption measures are recommended to protect Child Support Information classified as personal, sensitive, or confidential, per ISM 2103 Information and IT Asset Classification Standard. Applicable Organizations are advised to assess the risk to this

information and implement the following encryption practices where the risk assessment results warrant additional safeguards:

1. Encrypt when stored on workstations and servers.
2. Encrypt when transmitted over a private network.

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 2000 – Asset Protection Policy

ISM 2103 – Information and IT Asset Classification Standard

Section 5: References

SAM Section 5335.2 – Personal Computer Security

SAM Section 5345.2 – Cryptography

Health & Human Services Agency (CHHS) Encryption Policy, dated 9/27/2006

U.S Department of Health & Human Services/ACF, Automated System for Child Support Enforcement: A guide for states, June 2007

Section 6: Control and Maintenance

Owner: DCSS Information Security Office

Date Issued: January 16, 2007

Version: 2.0

Department of Child Support Services

INFORMATION SECURITY MANUAL		NUMBER: 2112
Document Type:	Standard	**EFFECTIVE:** 05-01-10
Subject:	Systems Acquisition, Development and Maintenance	
Synopsis:	Establishes requirements for incorporating security into Child Support information systems beginning at acquisition through development and maintenance.	

Section 1: Introduction

The California State Department of Child Support Services (DCSS) must ensure that information security is an integral part of critical information systems developed to automate the California Child Support Program, referred to as California Child Support Automated System (CCSAS), and provide for the integrity and security of information assets throughout the system development lifecycle (SDLC). Implementation of this standard for CCSAS is limited to DCSS Management as the entity responsible for the operation of CCSAS. For non-CCSAS critical systems, this standard shall be implemented by all Applicable Organizations. The purpose of this standard is to establish the following requirements for incorporating information security into information systems beginning at acquisition through development and maintenance.

- Information Technology (IT) Security Capital Planning
- System Development Life Cycle

Section 2: Standard Directives

2.1 IT Security Capital Planning

Applicable Organizations must consider integration of IT security into planning processes for systems used for purposes of administration or support of the California Child Support Program. This practice is consistent with industry best practices and ensures information security is well thought out in early stages of the IT SDLC and appropriate resources have been allocated for adequate protection of child support information systems.

2.2 System Development Life Cycle Requirements

All applicable child support systems and applications, whether in development or production, shall comply with information security requirements as defined in ISM 2105 Secure System, and include/implement appropriate security controls identified in NIST Special Publication (SP) 800-53. Information security activities shall be included in all phases of the SDLC, i.e. (1) Initiation, (2) Development and Acquisition, (3) Implementation and Assessment, (4) Operations and Maintenance, and (5) Disposal.

2.2.1 Initiation

This phase of the SDLC identifies and documents the need and purpose of a system and must include security planning and considerations. The security assessment and authorization

activities that support the security risk management process as defined in ISM 7000 Risk Management begin in this phase of the SDLC. Systems developed to support Child Support Services shall include, at minimum, the following activities during this phase:

1. System categorization and classification in accordance with ISM 2103 Information and IT Asset Classification, including the identification of any special handling requirements to transmit, store, or create information.
2. Security risk assessment of business requirements in terms of confidentiality, integrity, and availability of the Child Support System in accordance with ISM 7000 Risk Management to ensure threats, requirements, and potential constraints in security functionality and integration are considered.

2.2.2 Development and Acquisition

The development and acquisition phase of the SDLC focuses on secure system design based on findings of the risk assessment from the previous phase, and the system acquisition, development, and testing phase. Systems developed to support Child Support Services should include, at minimum, the following activities during this phase:

1. Evaluate and analyze identified risk in the initiation phase with the system's design, recommended solution, stated functional requirements, and the baseline security requirements to determine effectiveness of proposed solution to mitigate anticipated risks.
2. Document required security controls that should be implemented to assure appropriate level of protection (e.g., physical security, access control, auditing, network, etc.).
3. Implement security controls into system design.
4. Incorporate security requirements and/or security specifications for solicitation, contracts and/or purchase documents, either explicitly or by reference when conducting IT acquisitions.
5. Ensure acquisition agreements for services with external entities are in accordance with ISM 2109 Secure Data Transfer.
6. Perform testing and evaluation to ensure security measures are implemented as designed and to validate the effectiveness of the security controls.

2.2.3 Implementation and Assessment

The implementation and assessment phase of the SDLC includes the installation and evaluation of the system's performance in the operational environment. Procedures for security activities during this phase should be developed and implemented to include, at minimum, the following:

1. Incorporate scope of security testing in project work plan, including process for verification and validation of security control features prior to release to production and also within the operational environment upon post-implementation.
2. Ensure security control features can and do work correctly and effectively in the operational environment.
3. Obtain approval and authorization of system security prior to release to production/operation environment. This requires formal and documented security authorization from Applicable Organization's management, or designee for the information system to process, store, or transmit data.

2.2.4 Operations and Maintenance

The operations and maintenance phase of the SDLC is the period when the system is operating and in a production environment. This phase requires ongoing monitoring of system performance to ensure the system is performing as expected and that the security controls are working as designed. The system may require enhancements and/or modifications that may necessitate changes, addition and/or replacement of hardware and/or software. During this phase, systems developed to support Child Support Services shall include the following:

1. Processes and procedures for assured operations and continuous monitoring of the information system's security controls. This includes a plan of action and milestones for remediating compliance gaps and mitigating known risks, and performing security reauthorizations as required.
2. Management of system configuration and all changes in accordance with ISM 4100 Configuration Management.
3. Adequate and current system documentation and training for authorized personnel. System documentation must be appropriately secure and protected from unauthorized access and disclosure.
4. System monitoring for new or existing threats, vulnerabilities and risks, and implementation of appropriate measures to mitigate risks in accordance with ISM 3000 Threat Management, ISM 4000 Vulnerability Management, and ISM 7000 Risk Management.
5. Enforcement of the use of all software for Child Support Systems in accordance with all software license agreements with Child Support Services and copyright laws.
6. Enforcement of user rules of behavior as governed by ISM 5000 Acceptable Use Policy.
7. Routine preventative and regular maintenance (including repairs) of system components in accordance with manufacturer or vendor specifications and/or organizational requirements. This includes scheduling, performing, documenting and reviewing maintenance records.
8. Restriction of system maintenance activities to authorized personnel.
9. Control, approval and routine monitoring of the use of information system maintenance and remote maintenance tools on an ongoing basis.
10. Supervision of vendors and contractors at all times by authorized personnel when performing on-site maintenance or repairs. Refer to ISM 2100 Access Control, ISM 2108 Physical Security and ISM S-10-01 Media Protection and Sanitation.
11. Perform and test backup and retrieval processes, conduct operational recovery exercises (e.g., table top, simulation, etc.).
12. Manage security incidents in accordance with ISM 3100 Security Incident Management.

2.2.5 Disposal

The disposal phase of the SDLC is the final phase and provides for migration or disposal of a system, including closeout of any contracts in place. When Child Support Information Systems are transferred, become obsolete, or are no longer usable, it is important to ensure Child Support Information and IT Assets are protected and activities are conducted to securely and orderly terminate or migrate the system. Applicable Organizations shall include, where

applicable, the following key security activities for this phase of SDLC Child Support Information Systems:

1. Document the disposal/transition plan for closing or transitioning the system and/or its information.
2. Archive Child Support Information and/or records in accordance with applicable federal, state, and local records management requirements.
3. Sanitize (such as, clear, purge, or physical destruction) Child Support Information Systems in accordance with ISM S-10-01 Media Protection and Sanitation.

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 2105 – Secure System Standard

ISM 2103 – Information and IT Asset Classification

ISM S-10-01 – Media Protection and Handling

Section 5: References

SAM Section 4904 – Information Technology Five-Year Capital Plan

SAM Section 5320.5 – Classification of Information

SAM Section 5345 – Information Systems, Acquisition, Development, and Maintenance

ISO/IEC 27002:2005 (formerly 17799), Section 12 – Information Systems Acquisitions, Development and Maintenance

P1075, IRS Safeguards for Protection Federal Tax Returns and Return Information – Sections 3.2 Electronic Files.

NIST Pub 800-27 – Engineering Principles for IT Security (A Baseline for Achieving Security)

NIST Pub 800-37 – Guide for Security Certification and Accreditation for Federal Information Systems

NIST Pub 800-64 Revision 2 – Security Considerations in the Systems Development Life Cycle

NIST Pub 800-65 – Integrating IT Security into the Capital Planning and Investments Control Process

NIST Pub 800-60 – Guide for Mapping Types of Information and Information Systems to Security Categories

Section 6: Control and Maintenance

Owner: DCSS Information Security Office

Issued: May 1, 2010

Department of Child Support Services

INFORMATION SECURITY MANUAL	NUMBER:	2114
Subject: Wireless Communication Standard	**REVISED DATE:**	**09/24/2009**

Section 1: Introduction

Wireless communication provides portability, flexibility, and cost savings. However, if installed improperly, wireless technology can drastically increase information security risks to the organization's network. Insecure wireless installation may make Child Support Information and Child Support IT Assets vulnerable. This standard provides the following controls to secure wireless communications:

- Access Point Controls
- Wireless Client Controls

Section 2: Standard Directives

2.1 Access Point Controls

Applicable Organizations establishing and managing wireless network(s) must implement the following controls at their access points:

1. Secure the wireless router or access point administration interface; e.g. turn-off unnecessary services and ports, install latest security patches.
2. Encrypt wireless communication in compliance with ISM 2111 Encryption Standard.
3. Restrict connection privileges to authorized MAC addresses, where feasible.
4. Place access point hardware, including power and networking cables, at a secure location, to prevent intentional tampering or accidental disruptions. For example, recycling the power to the access point may make the unit vulnerable during system startup.
5. Limit the transmission of radio signals to the areas authorized for reception to prevent eavesdropping.
6. Configure Service Set Identifier (SSID) with an inconspicuous name and do not broadcast the SSID.
7. Disable wireless administration on access points.
8. Disable ad hoc mode access.
9. Establish wireless connection with a minimum of WPA version 2 using a randomly generated key length of at least 256 bits.

2.2 Wireless Client Controls

The following controls must be applied when a client device is wireless enabled. Applicable Organizations must ensure that these controls are applied automatically, when feasible. Otherwise procedures must be developed to instruct the user how to implement these controls:

1. Disable ad hoc mode to avoid unintentional association with unauthorized clients or access

points.

2. Disable wireless communication when client is connected to a wired network.
3. Install latest wireless patches; these patches are in addition to standard operating system patches.
4. Disable wireless communication when not needed.
5. Comply with ISM 2102 Remote Access Standard when connecting from outside the Applicable Organizations' network, over a wireless connection.
6. Activate firewall prior to connecting to a wireless network that is not managed by an Applicable Organization.

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 2000 – Asset Protection Policy

ISM 2102 – Remote Access Standard

ISM 2104 – Mobile Computing Standard

ISM 2111 – Encryption Standard

Section 5: References

NIST SP 800-97 – Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i

Section 6: Control and Maintenance

Owner: DCSS Information Security Office

Date Issued: January 16, 2007

Version: 2.0

Department of Child Support Services

INFORMATION SECURITY MANUAL	NUMBER:	2115
Subject: Separation of Duties Standard	**REVISED DATE:**	**09/24/2009**

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: Standard Directives

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, June 2007, 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 ISM 3100 Security Incident Management Standard.
7. Educate staff to identify and report potential conflicts between duties, responsibilities and authorities.

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 3100 – Security Incident Management Standard

ISM 2200 - Asset Protection Policy

Section 5: References

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

IRS Publication 1075 – Safeguards for Protecting Federal Tax Returns and Return Information, Access Control

Section 6: Control and Maintenance

Owner: DCSS Information Security Office

Date Issued: May 9, 2008

Version: 2.0

Department of Child Support Services

INFORMATION SECURITY MANUAL	NUMBER:	3000
Subject: Threat Management Policy	**REVISED DATE:**	**09/24/2009**

Section 1: Introduction

A Threat is an act or an event that has the potential to adversely impact Child Support Information and IT Assets, diminishing or preventing the Child Support Program from providing services to families. It is important for all Child Support Employees to recognize that threats are both technical and non-technical in nature and can range from employees leaking sensitive information to an external attacker trying to gain access to Child Support Information and Child Support IT Assets.

This DCSS Threat Management Policy contains the following policy directives:

- Threat Management Requirements
- Threat Monitoring Requirements
- Threat Mitigation Requirements

Section 2: Roles and Responsibilities

1. DCSS Management will establish a periodic reporting requirement for the DCSS CISO to measure the compliance and effectiveness of DCSS ISM policies and standards.
2. Applicable Organizations' Management will be responsible for implementing the requirements of DCSS ISM policies and standards.
3. Applicable Organizations' Management, in cooperation with the DCSS CISO, is required to train employees on DCSS ISM policies and standards.
4. Child Support Employees will comply with DCSS ISM policies and standards.

Section 3: Policy Directives

3.1 Threat Management Requirements

This directive lays the foundation for the Threat Management Program and establishes the management framework for monitoring, mitigating and preventing future threats to Child Support Information and IT Assets. Applicable Organizations' Management:

1. Supports the ongoing development and maintenance of the DCSS Threat Management Program.
2. Commits to the ongoing training and education of their staff responsible for the administration and/or maintenance of threat management controls or technologies. At a minimum, skills to be included or advanced include: incident response, attack trends and techniques, intrusion detection and prevention, secure System configuration, and security awareness.
3. Will use metrics to evaluate threats and measure the occurrence of threats attempting to impact the confidentiality, integrity or availability of Child Support Information and IT Assets.

The resulting threat profiles must incorporate data related to vulnerabilities and asset value to be effective. See Policies: ISM 7000 Risk Management Policy and ISM 2000 Asset Protection Policy.

4. Will evaluate these metrics to determine the need for additional controls or technologies capable of reducing the threat profile to Child Support Information and IT Assets.
5. Commits to establishing a formal review cycle for all threat management initiatives.
6. Will report security incidents to the DCSS CISO in compliance with ISM 3100 Security Incident Management Standard. Additional reporting requirements can be located within the Enforcement, Auditing and Reporting section of this policy.

3.2 Threat Monitoring Requirements

Threat monitoring commonly employs tools or techniques which are capable of detecting various types of activity associated with a potential attack or compromise. To ensure compliance with DCSS internal policies as well as applicable laws, regulations and State of California Policy, DCSS Management reserves the right to monitor and/or inspect all Child Support IT Assets. While threat monitoring is heavily reliant on the use of tools, the ability for Applicable Organizations' Management to respond to and recover from detected threats is of equal concern. This policy requires the creation and maintenance of appropriate and formally documented standards and procedures which will aid Applicable Organizations during the incident response and recovery process. Applicable Organizations' Management will:

1. Check appropriate System files for signs of wrongdoing and vulnerability exploitation at a frequency determined by both the criticality of the System involved and the severity of identified vulnerabilities. Frequency must consider the Child Support IT Asset's associated threat severity.
2. Review the following on a periodic basis:
   a. Appropriate threat monitoring tools are deployed.
   b. System logs and other files are inspected for signs of intrusion or intrusion attempts.
   c. Audit password strength and complexity to ensure compliance with ISM 2101 Password Standard.
   d. Occurrence and extent of virus infestations since prior review.
3. Utilize industry standard virus prevention technologies, techniques, and alerts.

3.3 Threat Mitigation Requirements

1. DCSS CISO will ensure that all DCSS ISM policies and standards conform to the requirements of the California State Administrative Manual and other relevant State and federal laws and regulations.
2. DCSS CISO will coordinate with Applicable Organizations' Management and other agencies as necessary to meet DCSS Management's responsibility for threat management.
3. DCSS Management will coordinate with Applicable Organizations' Management to meet threat management objectives.
4. DCSS Management will establish and maintain security incident handling procedures to facilitate reporting of security incidents by all Applicable Organizations' Management.
5. Applicable Organizations' Management will report security incidents in accordance with ISM 3100 Security Incident Management Standard.

6. DCSS CISO will cooperate with the State of California Information Security Officer and Applicable Organizations' Information Security Officers as necessary to meet their security objectives, and with California Highway Patrol for reporting and investigation of security incidents.

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 3100 – Security Incident Management Standard

Section 6: References

State Administrative Manual Section 5350 – Incident Management

Section 7: Control and Maintenance

Owner: DCSS Information Security Office

Date Issued: January 16, 2007

Version: 2.0

Department of Child Support Services

INFORMATION SECURITY MANUAL	NUMBER:	3100
Subject: Security Incident Management Standard	EFFECTIVE:	01/16/2007

Section 1: Introduction

DCSS Management is responsible for ensuring that security incidents that threaten Child Support Information and IT Assets are effectively managed to minimize damage and to prevent future incidents. This Security Incident Management Standard directs all Applicable Organizations to establish and maintain effective incident handling procedures and describes incident response and reporting requirements for Applicable Organizations.

This standard contains the following directives:

- Establishing Incident Response Procedures
- Criteria for Reporting Incidents
- Incident Reporting Requirements

Section 2: Key Terms and Definitions Applicable to this Standard

Security Incident – Any act or failure to act, or an event that creates a threat to the confidentiality, integrity and/or availability of Child Support Information and IT Assets, or person(s) or property located at any Child Support facility.

Child Support Information – Any information or state data, whether in the form of electronic media, physical document; data originated, taken or summarized from Child Support systems including all data collected, maintained or accessed through Child Support Services systems owned or administered by or on the behalf of the Child Support Services Program.

Personal Information – Any information classified as personal in accordance with ISM 2103, Information and IT Asset Classification Standard. 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; employee personnel records 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 Classification Standard. Examples include, but not limited to, Child Support participant application for Child Support Program 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.

Child Support Employee - An employee or contractor that works for any Applicable Organization that may have access to Child Support Information or Child Support IT Assets.

Section 3: Standard Directives

3.1 Establishing Incident Response Procedures

All Applicable Organizations must develop and maintain security incident management procedures consistent with this standard. Applicable Organizations' security incident management procedures must include descriptions of:

1. A central point of contact at the Applicable Organization for reporting of incidents.
2. A process for receiving, tracking, and referring incidents.
3. Roles and responsibilities for handling incidents.
4. Security incident resolution steps.
5. Management of communications during incident resolution.
6. Security incident documentation requirements.
7. Implementation of corrective actions.

3.2 Criteria for Reporting Incidents

In accordance with state and federal laws, certain items indicate what constitutes a security incident that must be reported. All Applicable Organizations and Child Support Employees shall report security incidents as described below to the DCSS ISO. Because there is no guarantee that a security incident will always conform to these criterion, all Applicable Organizations and employees shall always report suspicious activity to the DCSS ISO.

1. **Child Support Information** (includes electronic, paper, or any other medium)
    a. Theft, loss, damage, unauthorized destruction, unauthorized modification, or unintentional or inappropriate release of Child Support Information classified as personal or confidential.
    b. Possible acquisition of personal or confidential Child Support Information by unauthorized persons.
    c. Deliberate or accidental distribution or release of confidential or personal Child Support Information.
    d. Intentional or failures to act by an Applicable Organization or employees that threaten the confidentiality, integrity and/or availability of Child Support Information and IT Assets or violate Child Support Services policy.
2. **Inappropriate Use and Unauthorized Access** – This includes actions of Child Support Services employees and/or non-Child Support Services individuals that involve tampering, interference, damage, or unauthorized access to Child Support Information and Child Support Services systems. This includes, but is not limited to, successful virus attacks, web site defacements, server compromises, and denial of service attacks.
3. **Physical** – Theft, damage, destruction, or loss of Child Support Services Information Technology (IT) equipment, including laptops, tablets, integrated phones, personal digital assistants (PDA), or any electronic devices containing or storing Child Support Information; or planned or intentional acts to cause damage to DCSS property.
4. **Computer Crime** – Use of Child Support Services IT Assets in commission of a crime as defined in the Comprehensive Computer Data Access and Fraud Act.
5. **Any other incidents that violate Child Support Services policy**.

The DCSS ISO shall maintain all forms and documentation regarding security incidents reported to the DCSS ISO. All security incidents may be reported to the DCSS ISO either by telephone at (916) 464-5045 or via email at Info.Security@dcss.ca.gov. Refer to the DCSS form ASD-007 DCSS Information Security Event Report when reporting security incidents to the DCSS ISO.

3.3 Incident Reporting Requirements

All Child Support Employees shall report security incidents to the DCSS ISO that would place Child Support Information and Child Support IT Assets at risk. Reporting security incidents shall be in accordance with this Security Incident Management Standard and procedures established by Applicable Organizations.

Child Support Employees are required to report all security incidents as soon as practical, but no more than one (1) hour after a security event is detected.

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 3000 – Threat Management Policy

ISM 3102 – Virus Management Standard

Section 6: References

SAM Section 5350 – Incident Management

NIST SP 800-30 Risk Management Guide for Information Security

Civil Code sections 1798 et seq. – Information Practices Act of 1977

California Penal Code Section 502 – Comprehensive Computer Data Access and Fraud Act

Department of Child Support Services

INFORMATION SECURITY MANUAL	NUMBER:	3101
SUBJECT: DISASTER RECOVERY STANDARD	REVISED DATE:	09/24/2009

Section 1: Introduction

State Administrative Manual Section 5335 requires that state's essential services be restored as soon as possible and the applications which are most critical to the continuity of agency operations: remain in operation during the period of interruption; or, recover within acceptable timeframe for the business process. Furthermore, all systems that contain, use, process or support critical child support services must have a documented plan on how the organization would continue its mission and provide continuity of operations if service, use, or access was disrupted for an extended period of time.

This Disaster Recovery Standard contains the following standard directives:

- Federal Certification Requirements
- Business Continuity Requirements

Section 2: Standard Directives

2.1 Federal Certification Requirements

Each applicable organization must comply with the following requirements:

1. The State must have an approved disaster recovery plan which provides detailed actions to be taken in the event of a natural disaster (fire, water damage, etc.) or a disaster resulting from negligence, sabotage, mob action, etc. The disaster recovery plan should at a minimum include (1) documentation of approved backup arrangements, (2) Formal agreement of all parties that will be involved in the event of a disaster, (3) An established processing priority system, (4) Arrangements for use of a backup facility, and (5) Periodic testing of the backup procedures/facility. [1]
2. The system must have, or be supported by, an automated recovery and restore capability in case of system malfunction or failure. [2]
3. The State must conduct routine, periodic backups of all child support system data files, application programs, and documentation.[3]
4. The State must store duplicate sets of files, programs, documentation, etc., off-site in secure waterproof and fireproof facilities.[4]

---

[1] Automated Systems for Child Support Enforcement: A Guide for States, June 2007, requirement H-5a

[2] Ibid, requirement H-5d

[3] Ibid, requirement H-5e

[4] Ibid, requirement H-5f

2.2 Business Continuity Requirements

1. In compliance with the California State Administrative Manual 4843, Applicable Organizations must implement a process for developing and maintaining business continuity throughout the organization. A Business Continuity Plan (BCP) should be developed for each site or system. This will assist in a managed recovery of processing facilities, databases and services from a major disaster or system failure. The BCP should:
   - include measures to identify and manage risks
   - limit damage and interruption in the event of a disaster
2. A Business Continuity planning committee comprised of the Applicable Organization's Security Officer and Agency personnel must develop, test, and maintain the DCSS Business Continuity Plan to continue Child Support services in the event of a disaster that could disrupt normal operation. The plan should contain the following at the minimum:
   a. Identify and rank all mission critical services and applications according to priority and the maximum permissible outage for each critical application.
   b. Maintain inventory of all equipment and supplies and a floor plan of the current operating facility.
   c. Specify how frequently applications, data, software and databases are backed up and where they are stored off site.
   d. List the location of the alternate backup site.
   e. Prepare alternate site operating procedures.
   f. List the arrangement for delivery of backup data and software.
   g. Maintain updated contact information for all personnel involved in the recovery process.
   h. Identify the personnel designated to recover and sustain operations at the backup site; travel arrangements should be addressed if the backup site is not local.
   i. Identify recovery team members, identify primary and backup personnel and assign roles and responsibilities.
   j. Maintain contact information for all primary and backup personnel involved in the recovery process.
   k. Prepare recovery procedures.
   l. Prepare exercise procedures for the contingency plan.
   m. Identify the DCSS Business Continuity Plan as "confidential."
   n. Date each page of the plan.
   o. Exercise the plan annually or when a significant change occurs to the application.

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 2000 – Asset Protection

ISM 3000 – Threat Management Policy

Section 5: References

State Administrative Manual Chapter 5355 – Disaster Recovery Management

NIST SP 800-84 – Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities

U.S. Department of Health & Human Services/ACF, Automated System for Child Support Enforcement: A Guide for States, June 2007; ACF-H5

Section 6: Control and Maintenance

Owner: DCSS Information Security Office

Date Issued: January 16, 2007

Version: 2.0

Department of Child Support Services

INFORMATION SECURITY MANUAL	NUMBER:	3102
Subject: Virus Management Standard	**REVISED DATE**	**09/24/2009**

Section 1: Introduction

Virus Management is the process of preventing negative impacts to Child Support Information and/or IT Assets due to viruses. For the purposes of this standard, Virus is defined as any code or program (including macros and scripts) that is designed to cause damage to a user's computer, server, or computer network. This includes viruses, worms, trojans, spyware, etc.

Viruses may make computers processing and storing Child Support Information vulnerable to the compromise of confidentiality, integrity and availability of Child Support Information and IT Assets. Virus Management mitigates these risks and involves considerably less time and effort than responding to an exploitation event after one has occurred.

This standard contains the following Directives:

- Host Virus Protection Requirements
- Network Virus Protection Requirements
- Virus Infection Incident-Handling

Section 2: Standard Directives

2.1 Host System Virus Protection Requirements

The Applicable Organizations must apply following directives to all IT resources associated with Child Support Information:

1. All computer servers, workstations and laptops must have anti-virus software installed and resident in memory at all times.
2. All Child Support IT Assets must have the ability to confirm the installation of anti-virus software and compliance with the requirements described within this standard.
3. The anti-virus software must have the most current scan engine and virus definition file(s).
4. The anti-virus software must be capable of performing automatic updates to the scan engine and virus definition file(s).
5. The anti-virus software must be configured to:
   a. Start upon system boot-up.
   b. Automatically update scan engine and virus definition file(s).
   c. Prevent the user from modifying or disabling the anti-virus software.
   d. Remediate infected files by cleaning, deleting, or quarantining the file(s).
   e. Scan all files going into and out of the system.
   f. Perform a weekly scheduled scan of all files located on the hard-drive.

2.2 Network Virus Protection Requirements

Applicable Organizations must protect their network(s) that process or store Child Support Information. The following virus protection measures must be implemented in addition to the Host System Virus Protection Requirements (described above):

1. Install and configure anti-virus software at Internet gateway or firewalls to scan email attachments and other downloaded files.
2. Install anti-virus detection mechanisms to detect viruses traversing the internal networks. Upon detection of a virus, the system should disconnect the infected system from the network to prevent further infections and alert the system administrator.
3. Scan all portable media (e.g. floppy diskettes, CD's, USB drives, etc) when connected to the Applicable Organizations' network.

2.3 Virus Infection Management

For the purpose of this standard, an event or an activity resulting in compromise, corruption, or unavailability of Child Support Information and/or IT Assets caused by a malicious code is defined as a Virus Infection Incident. Applicable Organizations must implement following:

2.3.1 Virus Infection Incident Preparedness

1. Develop and exercise incident handling and incident response procedures for virus infection security incidents.
2. Employees must be trained on techniques for avoiding viruses e.g. don't open suspicious email, don't forward chain letters etc.

2.3.2 Virus Infection Incident-Handling

1. Immediately notify the DCSS CISO of any virus infection on systems that process or store Child Support Information. Refer to ISM 3100 Security Incident Management Standard.
2. Immediately contain the virus.
3. Remove or quarantine any infected computer or files until they can be verified as virus free.
4. Investigate how the file or system was infected and include this information in the ASD-700 Security Event Report Form.

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 Procedures

ISM 2000 – Asset Protection Policy

ISM 3000 - Threat Management Policy

ISM 3100 – Security Incident Management Standard

Section 5: References

SAM Section 5310 – Policy Management

NIST SP 800-40 – Creating a Patch and Vulnerability Management Program

Section 6: Control and Maintenance

Owner: DCSS Information Security Office

Date Issued: January 16, 2007

Version: 2.0

Department of Child Support Services

INFORMATION SECURITY MANUAL	NUMBER:	4000
Subject: Vulnerability Management Policy	**REVISED DATE:**	**09/24/2009**

Section 1: Introduction

Vulnerability is a flaw or weakness in a system's design, implementation, operation or management that could be exploited to violate the security in the system. Vulnerability Management is the discipline of monitoring and mitigating system vulnerabilities. Some examples of Vulnerability Management Activities are system scanning, system hardening and patch management.

This Vulnerability Management Policy contains the following policy directives:

- Vulnerability Management Requirement
- Vulnerability Monitoring Requirement
- Vulnerability Remediation and Mitigation Requirement

Together, these directives form the foundation of the DCSS Vulnerability Management Program.

Section 2: Roles and Responsibilities

1. DCSS Management will establish a periodic reporting requirement for the DCSS CISO to measure the compliance and effectiveness of DCSS ISM policies and standards.
2. Applicable Organizations' Management will be responsible for implementing the requirements of DCSS ISM policies and standards.
3. Applicable Organizations' Management, in cooperation with the DCSS CISO, is required to train employees on DCSS ISM policies and standards.
4. Child Support Employees will comply with DCSS ISM policies and standards.

Section 3: Policy Directives

3.1 Vulnerability Management Requirements

Vulnerability Management lays the foundation for the Vulnerability Management Program and establishes the management framework for monitoring, mitigating and preventing future vulnerabilities to DCSS assets.

1. DCSS Management supports the ongoing development and maintenance of the DCSS Vulnerability Management Program.
2. DCSS Management commits to the ongoing training and education of DCSS staff responsible for the administration and/or maintenance of DCSS Vulnerability Management controls or detection and mitigation technologies.
3. DCSS will maintain a Risk Management Plan that addresses risks to DCSS systems and those of Applicable Organizations.

4. Applicable Organizations' security staff will participate in the configuration management process to ensure changes to production systems do not introduce vulnerabilities.
5. DCSS will develop metrics to measure the occurrence of vulnerabilities, the effectiveness of mitigation efforts and any impacts to the confidentiality, integrity or availability of Child Support Information and Child Support IT Assets.
6. Child Support Employees will report security incidents pursuant to ISM 3100 Security Incident Management Standard for follow-up investigation. Additional Reporting requirements can be located within the Enforcement, Auditing and Reporting section of this policy.

3.2 Vulnerability Monitoring Requirements

Vulnerability monitoring commonly employs tools and processes capable of detecting and determining various types of vulnerabilities associated with a potential attack or compromise.

1. Applicable Organizations' Management will institute procedures to ensure that vulnerability assessments are performed periodically on systems that process or store Child Support Information.
2. Applicable Organizations' Management will establish vulnerability profiles based on the asset classification. Profiles are a set of security configurations.
3. Applicable Organizations' Management will conduct an initial vulnerability assessment to establish a baseline for each Child Support IT Asset and will utilize this baseline as the starting point for vulnerability metrics and the vulnerability management program. The baseline will be used to support the vulnerability remediation and mitigation processes.
4. Applicable Organizations' Management will use vulnerability profiles and baselines in the definition of requirements for deploying automated tools and manual processes.
5. Applicable Organizations' Management will conduct vulnerability assessments of systems that process or store Child Support Information, on a periodic basis according to each asset's classification.
6. The DCSS CISO in collaboration with Applicable Organizations' Management will prioritize and rate vulnerabilities according to the severity of the vulnerability, estimation of threat and asset classification.

3.3 Vulnerability Remediation and Mitigation Requirements

Applicable Organizations' Management will:

1. Utilize the findings from the vulnerability monitoring and assessment activities to plan for the ongoing elimination or mitigation of the vulnerabilities.
2. Track vulnerability mitigation to ensure that the vulnerability has been corrected, is scheduled for correction or risk documented and accepted according to risk assessment process.
3. Establish processes to ensure the tracking, enforcement and ability/authority of individuals responsible for corrective actions.
4. Cooperate with DCSS and outside agencies as necessary to meet its Vulnerability Management objectives. DCSS CISO will cooperate with the State of California Information

Security Officer as necessary to meet the security objectives of the state and the department.

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 4100 – Configuration Management Standard

ISM 4101 – Patch Management Standard

Section 6: References

SAM Section 5310 – Policy Management

NIST SP 800-40 – Creating a Patch and Vulnerability Management Program

Section 7: Control and Maintenance

Owner: DCSS Information Security Office

Date Issued: January 16, 2007

Version: 2.0

Department of Child Support Services

INFORMATION SECURITY MANUAL	NUMBER:	4100
Subject: Configuration Management Standard	**REVISED DATE:**	**09/24/2009**

Section 1: Introduction

The Configuration management establishes the process for controlling modifications to hardware, software, firmware, and documentation to ensure the information resources are protected against undocumented modifications before, during, and after system implementation. Configuration Management coordinates and informs customers and staff of all changes that impact any computing system or service (e.g. servers, network devices, etc.). Configuration Management Standard contains the following standard directives:

- Configuration Management Requirements
- Configuration Management Process Requirements

Section 2: Standard Directives

2.1 Configuration Management Requirements

The following Configuration Management standards must be implemented by applicable organizations:

1. Configuration Management procedures must be established to verify and validate changes to master files and application software.[1]
2. Configuration Management procedures must ensure that only authorized changes are made to the application software and that these changes are fully tested, approved, and migrated into production in a controlled manner, and documented to provide an audit trail of all system maintenance. [2]

2.2 Configuration Management Process Requirements

Applicable Organizations' Management will develop and maintain processes that meet the following requirements:

1. A formal written change request must be submitted for all changes, both scheduled and unscheduled.
2. A review of the request must be performed to determine any potential failures, and negative impact on any of the child support services.
3. All changes must be formally approved by the configuration management team before proceeding with the change.

---

[1] U.S. Department of Health & Human Services/ACF, Automated System for Child Support Enforcement: A Guide for States, June 2007, requirement H-3a

[2] Ibid, requirement H-3b

4. A Configuration Management Log must be maintained for all changes.
5. All configuration changes must be tested in the test environment prior to implementing into production.

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 4000 – Vulnerability Management Policy

Section 5: References

SAM Section 5335 – Communications and Operations Management

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

Section 6: Control and Maintenance

Owner: DCSS Information Security Office

Date Issued: January 16, 2007

Version: 2.0

Department of Child Support Services

INFORMATION SECURITY MANUAL	NUMBER:	4101
Subject: Patch Management Standard	**REVISED DATE:**	**09/24/2009**

Section 1: Introduction

This standard only applies to patches and patch levels relating to the protection of the confidentiality, integrity, and availability of Child Support Information and IT Assets.

Patch management is the process of controlling the deployment and maintenance of interim software releases into production environments. It helps to maintain operational efficiency and effectiveness, overcome security vulnerabilities, and maintain the stability of the production environment. Vulnerabilities are flaws that could be exploited to gain unauthorized access or control of a system and may result in the compromising of data and systems or the disruption of critical processing. Timely implementation of patches is critical to maintaining the confidentiality, integrity, and availability of information technology systems and involves considerably less time and effort than responding to an exploitation event after one has occurred.

This Patch Management standard directive contains the following sections:

- Patch Management Program Requirements
- Patch Management Process Requirements
- Patch Implementation Requirements

Section 2: Standard Directives

2.1 Patch Management Program Requirements

Applicable Organizations must ensure that all patches and patch levels relating to the confidentiality, integrity, and availability of Child Support Information and IT Assets are:

1. Assessed to determine priority and criticality based on the potential impact.
2. Implemented within the timeframes described in this standard in order to ensure that the patch level is “current” as defined by the product vendor. For example, all patches classified as “emergency” as described in section 2.3, must be applied immediately.
3. Applied to a connecting device that is not up-to-date prior to or immediately following the device being connected to the production network. If feasible, the device should only be allowed to access resources that are separate from the network that stores or processes Child Support Information.

   Note: When a patch for a known exploit is not available or devices cannot be patched, those devices must be protected through alternative mitigation efforts until a patch can be applied or the vulnerability no longer exists and the organizations Information Security Officer must be informed.

2.2 Patch Management Process Requirements

Applicable Organizations must develop, document, implement, and maintain a Patch Management Process that at a minimum includes the following:

4. A method to determine in a timely manner, the existing patch levels for all firmware and software used by the applicable organization.
5. A requirement that all patches must be obtained from authorized sources or supported vendors.
6. A documented change management process to ensure patches are approved and implemented in a controlled fashion.
7. Procedures and associated roles and responsibilities to:
   a. Monitor emerging threats and exploits, vulnerability announcements, patch notifications, and remediation solutions via www.us-cert.gov and vendor websites.
   b. Analyze and prioritize vulnerabilities to determine whether or not the patch should be implemented.
   c. Notify appropriate management of decision not to patch, if applicable.
   d. Log the patch priority and status.
   e. Test patches for compatibility with all system components prior to installation of the patch into production.
   f. Approve the patch.
   g. Implement the patch.
   h. Validate the patch has been properly implemented.

2.3 Patch Implementation Requirements

Applicable Organizations must use the following requirements to establish the priority of a patch. These requirements provide patch prioritization criteria, along with required implementation timeframes associated with each priority. However, if systems are already compromised, immediate action must be taken to remediate the exploit.

Priority	Criteria	Implementation Timeframe
Emergency	Organization is vulnerable, an exploit has been published and other organizations are being affected by the exploit.	Immediately
Critical	Organization is vulnerable, but no exploitation is known or exploitation is known but no organizations are being affected.	Within 1 week
Urgent	The vulnerable technology exists in the organization but vulnerability is difficult to exploit.	Within 2 weeks
Important	The vulnerable technology exists in the organization but the vulnerability is difficult to exploit and the risk to the confidentiality, integrity or availability of Child Support Information or IT Assets is limited or low.	Within 1 month
Not Applicable	The vulnerable technology does not exist in the applicable organization.	Not Applicable

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 4000 – Vulnerability Management Policy

Section 5: References

State Administrative Manual Section 5310 – Policy Management

NIST SP 800-40 – Creating a Patch and Vulnerability Management Program

Section 6: Control and Maintenance

Owner: DCSS Information Security Office

Date Issued: January 16, 2007

Version: 2.0

Department of Child Support Services

INFORMATION SECURITY MANUAL	NUMBER:	5000
Subject: Acceptable Use Policy	**REVISED DATE:**	**09/24/2009**

Section 1: Introduction

Child Support Information and IT Assets are strategic assets of the Department of Child Support Services (DCSS) and must be treated and managed as valuable resources. DCSS and Applicable Organizations provide various computer resources to their user community to enable users to perform their job-related duties. State law permits incidental access to State resources for personal use. This policy documents expectations for appropriate use of Child Support IT Assets. This Acceptable Use Policy is established to achieve the following:

1. To establish appropriate and acceptable practices regarding the use of Child Support IT Assets.
2. To ensure compliance with applicable State and federal law and other rules and regulations regarding the management of Child Support IT Assets.
3. To educate individuals who may use Child Support IT Assets regarding their responsibilities associated with computer resource use.

This Acceptable Use Policy contains the following policy directives:

- Acceptable Use Management
- Ownership
- Acceptable Use Requirements
- Incidental Use

Together, these directives form the foundation of the DCSS Acceptable Use Program.

Section 2: Roles and Responsibilities

1. DCSS Management will establish a periodic reporting requirement for the DCSS CISO to measure the compliance and effectiveness of DCSS ISM policies and standards.
2. Applicable Organizations' Management will be responsible for implementing the requirements of DCSS ISM policies and standards.
3. Applicable Organizations' Management, in cooperation with the DCSS CISO, is required to train employees on DCSS ISM policies and standards.
4. Child Support Employees will comply with DCSS ISM policies and standards.

Section 3: Policy Directives

3.1 Acceptable Use Management

1. DCSS Management supports the ongoing development and maintenance of the DCSS Acceptable Use Policy.

2. DCSS Management commits to the ongoing training and education of DCSS staff responsible for the administration and/or maintenance and/or use of Child Support IT Assets. At a minimum, basic Security Awareness training for all Child Support users must be conducted annually.
3. DCSS will use metrics to establish the need for additional education or awareness program measures in order to facilitate reduction in the threat and vulnerability profiles of Child Support IT Assets.
4. Applicable Organizations' Management will develop acceptable use procedures to protect Child Support IT Assets.
5. Any security issues discovered will be reported to the Information Security Officer or a designee of the Applicable Organization for follow-up investigation. Additional Reporting requirements can be located within the Enforcement, Auditing and Reporting section of this policy.

3.2 Ownership

Child Support Employees' use of Child Support Information and IT Assets is neither personal nor private. Authorized DCSS or Applicable Organization Security staff may access user access records at any time without knowledge of the user or owner. DCSS reserves the right to monitor and/or log all use of DCSS Information Resources with or without prior notice.

3.3 Acceptable Use Requirements

1. Users must report any perceived weaknesses in DCSS computer security to the appropriate security staff. Weaknesses in computer security include unexpected software or system behavior, which may result in unintentional disclosure of information or exposure to security threats.
2. Any user that observes any unauthorized access or misuse of any system that processes or stores Child Support Information or inappropriate use of any Child Support IT Asset must report the incident in accordance with the ISM 3100 Security Incident Management Standard.
3. Users must not deliberately attempt to access any data, documents, email correspondence, or programs contained on systems for which they do not have authorization.
4. Users must not engage in activity that may harass, threaten or abuse others or intentionally access, create, store or transmit material which may be deemed offensive, indecent or obscene, or that is illegal according to local, state or federal law.
5. Users must not engage in activity that may degrade the performance of information resources; deprive an authorized user access to Child Support IT Assets; obtain extra resources beyond those authorized; or circumvent DCSS computer security measures.
6. Child Support IT Assets must not be used for personal benefit, political activity, unsolicited advertising, unauthorized fund raising, or for the solicitation of performance of any activity that is prohibited by any local, state or federal law.
7. Users shall not violate copyright laws of copyrighted material and must not install any copyrighted software for which Applicable Organizations or the end user does not have an active license.

8. Users shall not install personally-owned copies of any software (including games, screensavers, Internet service programs, peer-to-peer file sharing, instant messaging programs, etc.).
9. Personally-owned information management devices shall not be connected to Child Support IT Assets. Information management devices include but are not limited to: Laptops, personal digital assistants (PDA), Blackberries, portable media (such as USB flash drives), or any other device that processes, stores, or transmits data.
10. Users must sign a statement that acknowledges reading and understanding information security policies and consequences of failure to comply.

3.4 Incidental Use

Government Code Section 8314 permits incidental personal use of state resources. At DCSS this means:

1. Incidental personal use of electronic mail, internet access, fax machines, printers, or copiers is restricted to DCSS approved users only and does not include family members or others not affiliated with DCSS.
2. Incidental use must not result in direct costs, cause legal action against, or cause embarrassment to DCSS.
3. Incidental use must not interfere with the normal performance of an employee's work duties.
4. Storage of personal email messages, voice messages, files and documents within DCSS's computer resources must be nominal.

DCSS Management will resolve incidental use questions and issues using these guidelines in collaboration with the DCSS CISO and DCSS Chief Counsel.

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 3100 – Security Incident Management Standard

ISM 6000 – Security Awareness Policy

Section 6: References

Government Code Section 8314
SAM Chapter 5325 – Human Resources Security
NIST SP 800-50 – Building an IT Security Awareness and Training Program
Government Code Section 8314

Section 7: Control and Maintenance

Date Issued: January 16, 2007
Owner: DCSS Information Security Office
Version: 2.0

Department of Child Support Services

INFORMATION SECURITY MANUAL	NUMBER:	6000
Subject: Security Awareness Policy	**REVISED DATE:**	**09/24/2009**

Section 1: Introduction

In order to achieve Child Support Program security goals, all Child Support Employees must understand the importance of information security as well as their individual responsibilities and accountability of information security. The Child Support Program must maintain an organizational culture that practices and values security and successfully communicates this message to employees and customers alike. The DCSS Security Awareness Program is a cornerstone for translating DCSS's security program vision into tangible results.

This Security Awareness Policy contains the following policy directives:

- Security Awareness Management Requirements
- Security Awareness Program Requirements

Together, these directives form the foundation of DCSS's Security Awareness Program.

Section 2: Roles and Responsibilities

1. DCSS Management will establish a periodic reporting requirement for the DCSS CISO to measure the compliance and effectiveness of DCSS ISM policies and standards.
2. Applicable Organizations' Management will be responsible for implementing the requirements of DCSS ISM policies and standards.
3. Applicable Organizations' Management, in cooperation with the DCSS CISO, is required to train employees on DCSS ISM policies and standards.
4. Child Support Employees will comply with DCSS ISM policies and standards.

Section 3: Policy Directives

3.1 Security Awareness Management Requirements

Security awareness provides the foundation for the DCSS Information Security Program.

1. DCSS Management supports the ongoing development and maintenance of the DCSS Security Awareness Program.
2. DCSS Management commits to the ongoing training and education of DCSS staff responsible for the administration and/or maintenance of the Security Awareness Program.
3. DCSS Management will use metrics to establish the need for additional education or awareness program measures in order to facilitate the reduction in the threat and vulnerability profiles of Child Support IT Assets.

3.2 Security Awareness Program Requirements

3.2.1 DCSS CISO's Requirements

The DCSS CISO will:

1. Prepare, maintain and distribute information security manuals that concisely describe DCSS information security policies and procedures.
2. Coordinate activities with Applicable Organizations' ISOs to promote security awareness among all Child Support Employees.
3. Coordinate activities with Applicable Organization's ISOs to develop a security awareness training program.
4. Coordinate with Applicable Organizations' ISOs to develop methods and metrics to measure the initial security awareness baseline and subsequent employee awareness to determine the effectiveness of training. These methods may include use of, sample awareness testing, and subsequent post training surveys.
5. Develop and maintain a communications process to inform Child Support Employees of new computer security program information, security bulletin information, and security items of interest.

3.2.2 Applicable Organizations' Management Requirements

Applicable Organizations' Management will:

1. Provide security awareness training to all Child Support Employees prior to, or at least within 30 days of being granted access to any Child Support Information or Child Support IT Assets. Training may be provided via classroom training, a computer-based training application, or reading of security awareness manuals/handouts.
2. Provide refresher security awareness training annually to all Child Support Employees.
3. Develop a process to ensure that Child Support Employees' attendance at the required security awareness training is tracked.
4. Encourage Applicable Organizations' security staff to participate in the activities of information security professional organizations such as Information Systems Security Association, (ISSA) and provide feedback on successful security awareness presentations and programs.
5. Ensure that any contract with a service provider, that requires the service provider's employees to obtain access to Child Support Information or Child Support IT Assets, contains a requirement for its employees to complete security awareness training and sign a confidentiality statement provided by the Applicable Organization.

3.2.3 Child Support Employees Requirements

All Child Support Employees will:

1. Attend all required security awareness training and sign a confidentiality statement.
2. Comply with DCSS ISM policies and standards.

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 1000 – Information Security Policy

ISM 5000 – Acceptable Use Policy

Section 6: References

SAM Section 5325 – Human Resources Security

NIST SP 800-50 – Building and IT Awareness and Training Program

NIST SP 800-16 – IT Security Training Requirements: A Role and Performance Based Model

Section 7: Control and Maintenance

Owner: DCSS Information Security Office

Date Issued: January 16, 2007

Version: 2.0

Department of Child Support Services

INFORMATION SECURITY MANUAL	NUMBER:	7000
Subject: Risk Management Policy	**REVISED DATE:**	**09/24/2009**

Section 1: Introduction

Risk is the net negative impact of the exercise of vulnerability, considering both the probability and impact of occurrence. Risk Management is the process of identifying risk, assessing risk and taking steps to reduce risk to an acceptable level. DCSS has the responsibility of maintaining the confidentiality, integrity and availability of Child Support Information and IT Assets. To achieve this goal, it is essential that DCSS implement a Risk Management Program. This Risk Management Policy contains the following Directives:

- Risk Management Requirements
- Risk Assessment Requirements
- Risk Mitigation Requirements

Section 2: Roles and Responsibilities

1. The DCSS CISO will provide leadership, guidance and will collaborate with Applicable Organizations' Management to implement the requirements of this policy and underlying standards.
2. DCSS Management will establish a periodic reporting requirement for DCSS's CISO to measure the compliance and effectiveness of this policy within DCSS and the Applicable Organizations.
3. Applicable Organizations' Management, in cooperation with the DCSS CISO, is required to train employees on DCSS ISM policies and standards.
4. All Child Support Employees are required to comply with this policy.

Section 3: Policy Directives

3.1 Risk Management Requirements

Risk Management establishes the framework for identifying, assessing and mitigating risks to Child Support Information and IT Assets.

1. DCSS Management supports the ongoing development and maintenance of the DCSS Risk Management Program.
2. DCSS Management commits to the ongoing training and education of DCSS staff responsible for the administration and/or maintenance of DCSS Risk Management controls or detection and mitigation technologies.
3. DCSS CISO will maintain a documented Security Plan with plan of action and milestones that addresses risk management for Child Support Information and IT Assets and implement procedures.

4. The DCSS CISO will ensure that risk assessments are performed at a minimum every two years and upon significant changes to systems that process or store Child Support Information.[1]
5. Applicable Organizations will assign security staff to participate in the configuration management process to ensure changes to production systems do not introduce risks to Child Support IT Assets.
6. DCSS CISO will develop metrics to measure the occurrence of risks, the effectiveness of mitigation efforts and any impacts to the confidentiality, integrity, or availability of Child Support Information and Child Support IT Assets.
7. Child Support Employees will report security incidents pursuant to ISM 3100 Security Incident Management. Additional Reporting requirements can be located within the Enforcement, Auditing and Reporting section of this policy.

3.2 Risk Assessment Requirements

1. The DCSS CISO will develop a Risk Assessment methodology including continuous monitoring and comprehensive security controls reviews and assessments.
2. Applicable Organizations' Management will cooperate with the DCSS CISO and support risk assessment activities.

3.3 Risk Remediation and Mitigation Requirements

Applicable Organizations Management will:

1. Utilize the findings from the risk monitoring and assessment activities to plan for the ongoing elimination or mitigation of the vulnerabilities.[2]
2. Track risk mitigation activities to ensure that corrective action has been taken or is scheduled to be taken. If no corrective action is taken, then acceptance of the risk will be documented.
3. Authorize individuals to conduct corrective actions.
4. Interact with outside agencies and other organizations as necessary to meet its Risk Management objectives. DCSS CISO will cooperate with the State of California Information Security Officer as necessary to meet the security objectives of the state and the department.
5. Consider the value of the asset and its impact on the department's services and cost of implementing mitigation measures.

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

[1] Automated Systems for Child Support Enforcement: A Guide for States, June 2007, Requirement H-1c

[2] Ibid, Requirement H-1

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 4100 – Configuration Management Standard

Section 6: References

SAM Section 5305 – Risk Management

NIST SP 800-53A – A Guide for Assessing Security Controls

Section 7: Control and Maintenance

Owner: DCSS Information Security Office

Date Issued: January 16, 2007

Version: 2.0

Appendices

THIS PAGE IS INTENTIONALLY LEFT BLANK

INFORMATION SECURITY EXCEPTION REQUEST

DCSS ISM 1300 (07/25/07)

DCSS Information Security policies and standards are developed and implemented to best protect Child Support Information and Child Support IT Assets. Exceptions to the policies may increase security risks, yet may be justified under certain circumstances. The purpose of the Exceptions process is to ensure that all exceptions from DCSS Information Security policies and standards are assessed for potential security risks and that mitigation strategies are implemented where applicable.

Please complete all areas of requested information. This form must be signed by the applicable organization's manager or child support information/IT asset owner requesting the exemption. Submit the completed form to:

The Department of Child Support Services
Attn: Information Security Office
P. O. Box 419064
Rancho Cordova, CA 95741-9064

1. Please list the number and name of the DCSS Information Security Manual (ISM) policy or standard for which the exception(s) is requested. Multiple requests may be submitted as a single request when there is a common underlying reason.

DCSS Policy/Standard	DCSS Policy/Standard Name

2. Enter the length of time for which the exception(s) is requested and the implementation date.

Duration of Exemption	Implementation Date

3. Scope of requested exception(s): Organizational unit to which the exception(s) will apply (for example, will the exception apply to the entire Applicable Organization, specific working units, or individuals or systems within the organization?)

Physical locations(s) to which the exception(s) will apply.

Logical address(es) to which the exception(s) will apply.

4. Give a description of the technical or business need for each requested exception. This should be a detailed explanation of what each exception entails. Include a description of each of the following:

How would the identified DCSS ISM policy or standard be modified to meet your business needs?

What is the business or technical need for this exception(s)?

What will the impact on business processes, system functionality, or technical quality if the exception(s) is not granted?

What costs will be incurred if the exception(s) is not approved?

If the exception(s) is approved, will there be any security risk to Child Support information and/or IT assets? If the answer is yes, explain below.

Describe safeguards that will be implemented to reduce the security risks introduced due to the exception(s).

5. Provide the requestor's contact information below.

Name of the Organization

Contact Name | Contact Title

Phone Number | Email Address

6. Signature of applicable organization's manager or Child Support/IT asset owner requesting the exception(s).

Name of Approving Authority	Title
Phone Number	Email Address
Signature	Date

THIS SECTION IS FOR THE USE OF THE DEPARTMENT OF CHILD SUPPORT SERVICES, INFORMATION SECURITY OFFICE

7. Approval/Rejection details.

Details of Approval /Rejection

Approval	Disapproval

Details

Conditions

Projected Review Date

Submit

DCSS ISO Use Only
Security Event/Incident No.
_____

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)

DCSS ISO Use Only
Security Event/Incident No.
_____

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 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.

THIS PAGE IS INTENTIONALLY LEFT BLANK

Guidelines

THIS PAGE IS INTENTIONALLY LEFT BLANK

Department of Child Support Services

INFORMATION SECURITY MANUAL		NUMBER: G-09-01
Document Type:	Guideline	**EFFECTIVE:** 09-23-09
Subject:	Training with Privacy Protection	
Synopsis:	Provides recommendations and guidance for maintaining privacy protection when providing training.	

1.0 Purpose

The purpose of this document is to provide guidelines to Department of Child Support Services (DCSS) and local child support agencies (LCSAs) for maintaining privacy protection of its customers and employees when providing training.

2.0 Definitions

Personal Information – Any information that is maintained by an agency that identifies or describes an individual, including but not limited to, his or her name, Social Security number, physical description, home address, home telephone number, education, financial matters, and medical or employment history. It includes statements made by, or attributed to, the individual.

Notice-Triggering Personal Information – An individual's first name <u>or</u> first initial <u>and</u> last name in combination with any one or more of the following data elements:

(1) Social Security number.
(2) Driver's License number or California Identification Card number.
(3) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.
(4) Medical Information (as defined in Civil Code section 1798)
(5) Health Information (as defined in Civil Code section 1798)

De-identified Personal Information – Information that does not identify any individual and there is no reasonable basis to believe that the information can be used to identify an individual.

3.0 Guideline

It is the recommendation of the DCSS Information Security Office to avoid the display or distribution of personal information to honor the privacy of our customers by limiting the use of personal information in any training material; and reduce the risk of violating any state or federal privacy laws or conflicts of interest. Although it may not be feasible to partially or completely eliminate the use of personal information in training demonstrations, listed below are guidelines for training DCSS and LCSA personnel that will reduce risks to potential exposures. These guidelines are provided with the assumption that all participants in the training have received security awareness training and have signed confidentiality statements on file.

> **TIP**: *If you think about replacing the information displayed with **your** information and get a queasy feeling, you may be displaying too much information.*

1. **Webcast Training**. Personal information may be displayed with the assurance that:

a. No non-DCSS or non-LCSA persons can log into the webcast. (This may require some technical requirements or assistance.)
b. Training attendance must be controlled and restricted only to DCSS or LCSA personnel. No other persons should be permitted to attend.
c. Privacy and confidentiality disclaimer should be displayed prior to and/or during the training session.
d. Considerations for conflict-of-interest cases should be addressed when choosing cases for training and DCSS or LCSA employees should not be included.

Note: It is recommended that all training be conducted outside of the production environment.

2. **Classroom Training**. Personal information may be displayed (e.g. within a PowerPoint presentation) with the assurance that:
   a. Training attendance is controlled and restricted only to DCSS or LCSA personnel. No other persons should be permitted to attend.
   b. Privacy and confidentiality disclaimer should be displayed prior to and/or during the training.
   c. Considerations for conflict-of-interest cases should be addressed when choosing cases for training and DCSS or LCSA employees should not be included.

   Note: In **all** cases where non-DCSS or non-LCSA participants view any personal information (e.g., in the Practice Environment), they **must** sign non-disclosure forms.

3. **PowerPoint Presentations**.
   a. For DCSS and LCSA personnel training, screen-shot images should be presented with redacted (made unreadable) or limited personal information. If the use of personal information is included, always redact any Social Security numbers and Drivers License numbers. The use of 'dummy information' (e.g., Jane Doe at 123 Main Street, Anywhere, CA, SSN: 123-45-6789 or ###-##-####) is also an alternative. Case numbers are not considered personal or confidential information unless it is used in combination with any required security code, access code, or password that would permit access to an individual's information.
   b. Display a privacy and confidentiality disclaimer prior to and/or during training sessions where personal information is displayed.
   c. Restrict training attendance to DCSS and LCSA personnel where personal information is displayed.
   d. For non-DCSS and non-LCSA personnel PowerPoint presentations, either avoid the use of any personal information in the training material or use only dummy information.
   e. Considerations for conflict-of-interest cases should be addressed when choosing cases for training and DCSS or LCSA employees should not be included.

4. **Practice Environment**
   a. No non-DCSS or non-LCSA persons can log into the webcast. (This may require some technical requirements or assistance.)
   b. Training attendance must be controlled and restricted only to DCSS or LCSA personnel. No other persons should be permitted to attend.
   c. Privacy and confidentiality disclaimer is displayed prior to and/or during the training.

d. Considerations for conflict-of-interest cases should be addressed when choosing cases for training and DCSS or LCSA employees should not be included.

Note: In **all** cases where non-DCSS or non-LCSA participants view any personal information (e.g., in the Practice Environment), they **must** sign non-disclosure forms.

5. **Training Material**. All classroom documents and handouts must either avoid the use of personal information in the training material or use "dummy information" (e.g., Jane Doe at 123 Main Street, Anywhere, CA, SSN: 123-45-6789 or ###-##-####) or not contain personal information. Case numbers are not considered personal or confidential information unless it is used in combination with any required security code, access code, or password that would permit access to an individual's information.

4.0 Related Policies and Standards

ISM 1000 – Information Security Policy

ISM 2103 – Information and IT Asset Classification Standard

5.0 References

IRS Publication 1075 – Sections 4.7.3, 5.6.3, 6.2, 6.3, and 7.2.9

SAM 5300 – Information Security (Office of Information Security and Privacy Protection)

Department of Child Support Services

INFORMATION SECURITY MANUAL		NUMBER: G-09-02
Document Type:	Guideline	**EFFECTIVE:** 09-23-09
Subject:	Security Awareness Training	
Synopsis:	Guidelines to implement information security awareness training.	

1.0 Purpose

The purpose of this document is to provide local child support agencies (LCSAs) with an overview of the information security training program and guidelines for implementation.

2.0 Guideline

As part of its commitment to ensuring the financial and health security of children across California, the Department of Child Support Services (DCSS) Information Security Office established an Information Security Awareness Program. The focus of the information security training is to communicate the information security policies, roles and responsibilities, and ramifications for noncompliance to those individuals who access Child Support information. The major attributes of the information security program are detailed below:

- Security awareness training should be provided to all employees upon employment with child support services and annually thereafter to meet child support services security awareness training requirements.
- Training should contain instructional components, such as, but not limited to, the confidential nature of child support information, laws and regulations governing child support information, user responsibility for protecting child support information, and the consequences and legal liability of unauthorized access to or disclosure of child support information.
- Awareness training may be in any form, whether it be video, PowerPoint, computer-based training (CBT), etc., as long as it contains all the security awareness training components as required by DCSS. Training material developed by DCSS is available on the CA Child Support Central as an option for LCSAs use to meet DCSS training requirements.
- Security awareness training for new employees requires each employee to sign a Confidentiality Statement (DCSS 0593) and a UNAX Certification (DCSS 0570). These forms must be maintained locally.
- Annual security awareness training requires employees to sign an Acknowledgement of Understanding (ASD-011) or a form equivalent to the ASD-011 upon completion of annual security awareness training. These forms may be maintained locally or submitted to the DCSS ISO for retention. (Note: DCSS provided CBT security awareness training incorporates the requirement for the signing and retention of an ASD-011.)

- Each LCSA should maintain any of its own developed training materials and documentation.

The Federal Internal Revenue (IRS) publishes a training video that provides security awareness and disclosure training requirements that specifically relate to federal tax information (FTI) access and disclosure. The IRS training video *may* be provided to employees as a supplement to or part of their initial and/or annual training. However, the IRS video may *not* be used as a replacement for DCSS developed security awareness training. DCSS security awareness training relates to all child support information, including FTI, or any other confidential or personal information that requires protection by all federal or state laws. The DCSS security awareness training meets both IRS and State requirements for initial and annual awareness training.

3.0 Related Policies and Standards

ISM 1000 – Information Security Policy

ISM 6000 – Security Awareness

4.0 References

IRS Publication 1075 – Sections 4.7.3, 5.6.3, 6.2, 6.3, and 7.2.9

SAM 5300 – Information Security (Information Security and Privacy Protection)

Department of Child Support Services

INFORMATION SECURITY MANUAL		NUMBER: G-10-01
Document Type:	Guideline	**EFFECTIVE:** 05-01-10
Subject:	Media Sanitation	
Synopsis:	Recommended sanitation guidelines for media.	

1.0 Purpose

This guideline provides technical assistance for sanitation of any media used to process or store Child Support Information. When selecting the method and mechanism for media sanitation, consideration should be given to the categorization of the information along with factors such as the type and size of the media, and who has physical control of the media.

The IRS Publication 1075, Tax Information Security Guidelines for Federal, State and Local Agencies and Entities, requires the use of moderate impact level categorization as described in Federal Information Processing (FIPS) 199 and the associated moderate security controls from the National Institute of Standards and Technology (NIST) Special Publication 800-53 for all media used to store or process federal tax information (FTI). These security controls should be used to drive decisions regarding media sanitation. Refer to DCSS ISM 2110, Media Protection and Sanitation.

2.0 Sanitation Methods

Media includes both digital (e.g., diskettes, magnetic tapes, hard drives, flash/thumb drives, compact disks, digital video disks) and non-digital media (e.g., paper, microfilm). Media may be contained in various systems or devices, such as, desktop PC's, notebooks, computers, servers, mainframes, multi-function printer/copier/fax, network devices, security devices, as well as other digital devices. There are three methods of media sanitation listed in Table 1 below, each appropriate for different situations and each provide varying levels of protection for the confidentiality of the information contained on the media.

Table 1

Method	Description	Examples
Clearing	Protects confidentiality of Child Support Information against keyboard attacks, which is data scavenging or retrieval through the use of software/data file recovery utilities or tools. Any overwriting or disk "wiping" utility that use Department of Defense compliant software is an acceptable method of clearing.	DBAN (http://www.dban.org/) White Canyon (http://www.whitecanyon.com/index.php)

Method	Description	Examples
Purging	Protects confidentiality of information against laboratory attack, which is data scavenging or retrieval through laboratory means. This typically involves the use of signal processing equipment and specially trained personnel. Executing the secure erase firmware command on a disk is an acceptable method of purging.	Sanitizing hard drives at the hardware level with Secure Erase Utility http://cmrr.ucsd.edu/people/Hughes/SecureErase.shtml Note: Tapes are capable of being purged for re-use with the use of degaussers. Degaussing hard drives typically renders the drive useless. Refer to "Degaussers" under the Destroying method of this table.
Destroying	The ultimate form of sanitation is to physically destroy the media. Physical destruction can be accomplished using a variety of methods with the objective of making the data unrecoverable or unable to be reconstructed. Optical media (e.g., CDs, DVDs) must be destroyed by pulverizing, shredding or incineration. Use of a certified degausser is also an acceptable method of destroying electronic media. Degaussing is not effective for optical media (e.g., CDs, DVDs).	For hard drives, any method of disrupting the full revolution of the hard drive platter is acceptable. Examples include drilling through hard drive platter, grinding platter with a sand grinder, hammering railroad spike through platter, etc. Optical mass storage media, including compact disks (CD, CD-RW, CD-R, and CD-ROM), optical disks (DVD), and magneto-optic (MO) disks should be destroyed by pulverizing, cross-cut shredding, or burning. Paper shredders can be used to destroy flexible media such as diskettes once the media are physically removed from their outer containers. The shred size of the refuse should be small enough that there is reasonable assurance that the information cannot be reconstructed. Degaussers: See approved list of degaussers evaluated and provided by the National Security Agency (NSA) in the document "Evaluated Products List - Degausses" dated March 2009." The degausser must be able to produce at least 5000 *oersteds* to be able to erase both Longitudinal and Perpendicular storage devices manufactured after year 2004. http://www.nsa.gov/ia/_files/government/MDG/EPL-Degausser30March2009.pdf Shredders: See approved list of shredders evaluated and provided by NSA in the document "Evaluated Products List – High Security Crosscut Paper Shredders" dated April 2009." http://www.nsa.gov/ia/_files/government/MDG/NSA_CSS-EPL-02-01.pdf

Method	Description	Examples
		IRS P1075 requires paper shredded to effect 5/16" wide or smaller strips; microfilm and microfiche shredded to effect a 1/35- inch by 3/8- inch strips. If shredding is part of the overall destruction of FTI, strips can in effect be set at the industry standard (currently ½"). However, when deviating from 5/16", FTI in this condition (i.e., strips larger than 5/16"), must be safeguarded until it reaches the stage where it is rendered unreadable.

The NIST SP 800-88 provides guidance listed below in Table 2 for sanitation on different types of removable media. Procedures and/or equipment should be tested at least annually, where applicable. Specific standards and products can be found in the National Security Agency/Central Security Service (NSA/CSS)-approved product lists at: http://www.nsa.gov/ia/guidance/media_destruction_guidance/index.shtml.

When confronted with an unfamiliar circumstance or if not certain of appropriate action, contact the DCSS ISO for assistance at info.security@dcss.ca.gov.

Table 2

Media Type	Clear	Purge	Destroy
Floppy Disks	Overwrite	Degauss using a NSA/CSS approved degausser	Incinerate or shred
ATA Hard Drives	Overwrite	Secure Erase	Disintegrate, pulverize, incinerate, degauss, or dissembled and degauss the enclosed platters using a NSA/CSS approved degausser
SATA Hard Drives	Overwrite	Secure Erase	Disintegrate, pulverize, incinerate, degauss, or dissembled and degauss the enclosed platters using a NSA/CSS approved degausser
SCSI Drives	Overwrite	Secure Erase	Disintegrate, pulverize, incinerate, degauss, or dissembled and degauss the enclosed platters using a NSA/CSS approved degausser
USB Removable Drives	Overwrite	Secure Erase	Disintegrate, pulverize, incinerate, degauss, or dissembled and degauss the enclosed platters using a NSA/CSS approved degausser
Zip Disks	Overwrite	Degauss using a NSA/CSS approved degausser	Incinerate or shred

Media Type	Clear	Purge	Destroy
Magnetic Tapes	Overwrite	Degauss using a NSA/CSS approved degausser	Incinerate or shred
CDs/DVDs	N/A	N/A	Optical disk grinding device, incinerate, shred.
Paper and microfilms	N/A	N/A	Incinerate or shred

3.0 Sanitation Requirements

Each of the three methods of media sanitation appropriate for Child Support Services Program organizations should be used for different environmental factors, such as type of media, size of media, and who has control of the media. Listed in the Table 3 below are recommended actions for systems or devices that contain media with Child Support Information.

Table 3

	Description	Clear	Purge	Destroy
Internal Re-Use	Media for re-use within the Child Support Services	✓	✓	
Surplus Re-Use	Media for re-use outside of Child Support Services		✓	✓
Onsite Repair	Media for repair onsite of Child Support Services – use non-disclosure/confidentiality agreements for vendor (if applicable).			
Offsite Repair	Media for repair offsite of Child Support Services – use non-disclosure/confidentiality agreements for vendor (if applicable). Degauss or physically destroy hard drives for hard drive exchanges.		✓	
Surplus Disposal	Media that is obsolete or no longer required.		✓	✓

Vendor Repairs

If repairs are performed by a vendor, be sure the vendor is a certified contractor and that all the necessary signed contracts and/or agreements are in place. Agreements should include and clearly identify contracted sanitation methods and/or security provisions. Require and obtain from vendor a validation of completion of the contracted activity (e.g., certify and document successful sanitation and media tracking information such as hard drive serial number, make, model, type of sanitation, date, printed name of the person performing the task and their signature). All sanitation of media containing Child Support Information must be witnessed by a Child Support Employee (as defined in the ISM).

Certification of Sanitation

Document and certify all media destruction via a log on paper, spreadsheet, database or some form of tracking mechanism and maintain for at least six (6) years. Record information in the log, such as, the media item, model number, serial number, asset tag number (if applicable), method of sanitation/destruction, date of destruction, etc.

4.0 Related Policies and Standards

Media Protection and Sanitation Standard – ISM 2110

NIST SP 800-88 – Media Sanitation Guideline

National Security Agency (NSA)/Central Security Service (CSS) Storage Device Declassification Manual

NSA/CSS Media Destruction Evaluated Product Lists

5.0 References

California Civil Code Section 1798 (Information Practices Act)

IRS P1075, IRS Safeguards for Protecting Federal Tax Returns and Return Information – Sections 4.6 Physical Security of Computers, Electronic, and Removable Media; 7.2.7 Disposal; 8.3 Destruction Methods; and 8.4 Disposing FTI-Other Precautions