Information Security Manual

Supporting California's Children

August 2007

Information Security Office
California Department of Child Support Services

THIS PAGE IS INTENTIONALLY LEFT BLANK

DCSS Information Security Manual

Information Security Manual

THIS PAGE IS INTENTIONALLY LEFT BLANK

Department of Child Support Services

INFORMATION SECURITY MANUAL	**NUMBER:**	**1000**
Subject: Introduction	**REVISED DATE:**	**Original**

Section 1: Introduction

1.1 DCSS Information Security Office

The Department of Child Support Services (DCSS) administers the California Child Support Program. 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.

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 Chief Information Security Officer (CISO) to manage the Information Security Office and the Information Security Program. Guidance, direction, and authority for information security is centralized and coordinated under the direction of the CISO. Therefore, the CISO has delegated authority to implement appropriate oversight and assurance procedures to ensure DCSS employees and applicable organizations comply with Information Security Program requirements.

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

The DCSS ISO provides information security related guidance, oversight, education, and enforcement for the California Child Support Program and is responsible for the development, implementation, maintenance, and enforcement of the CA Child Support *Information Security Program*.

1.2 DCSS Information Security Program

The DCSS Director approves, sponsors, and supports the Information Security Program and has established the Information Security Office (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 : ensuring that information is accessible only to those authorized to have access;
- integrity: safeguarding the accuracy and completeness of information and processing methods;
- availability: ensuring that authorized users have access to information and associated assets when required.

CA Child Support Program Management is expected to remain committed to taking appropriate actions to mitigate, respond to and recover from identified vulnerabilities and threats.

The Information Security Office maintains an Information Security Awareness Program to ensure the Information Security Manual is properly communicated to the California Child Support Program.

DCSS's Information Security program will also develop policies, standards, guidelines and procedures to provide for the operational recovery and business continuity of the California Child Support Program.

1.3 Information Security Manual

The DCSS Information Security Program uses a risk management approach to develop and implement the Information Security Manual (ISM), a compilation of policies, standards, guidelines, and procedures that address security objectives in concert with business and operational needs. The DCSS Information Security Manual (ISM) is the foundation of the Information Security Program for the California Child Support Program. Consequently, all individuals having access or responsibility to manage California Child Support Information and Child Support IT Assets are required to comply with the DCSS ISM. Because, the responsibility for Information Security is shared among multiple organizations, this DCSS ISM provides not only directives, but also describes which organization is responsible for carrying out those directives.

Section 2: How to Use This Manual

The DCSS ISM is produced for use by all individuals with 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 employee 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 DCSS ISM 1301 Definitions. These defined terms apply to all sections of this DCSS ISM. All defined words throughout this DCSS ISM are capitalized.

The DCSS ISM is intended to incorporate the requirements of Chapter 4800 of the California State Administrative Manual, Federal laws, and the Office of Child Support Enforcement (OCSE), Office of Information Systems Management, Information Memorandum 93-1. The ISM identifies the minimum steps necessary, however all those with access to California Child Support Information and Child Support IT Assets should exercise additional ‘due diligence’ in ensuring the protection of information and assets. This may include implementing additional measures to protect Child Support Information and Child Support IT Assets.

The DCSS ISM consists of six policies. Within each policy are related standards, procedures and forms.

Chapter	Includes Sections
1000 Introduction	1200 Exception Request Procedure 1300 Exception Request Form 1301 DCSS ISM Definitions
2000 **Asset Protection Policy**	2100 - 2199 Asset Protection Standards 2200 - 2299 Asset Protection Procedures 2300 - 2399 Asset Protection Documents 2400 - 2499 Asset Protection Guidelines
3000 **Threat Management Policy**	3100 - 3199 Threat Management Standards 3200 - 3299 Threat Management Procedures 3300 - 3399 Threat Management Documents 3400 - 3499 Threat Management Guidelines
4000 **Vulnerability Management Policy**	4100 - 4199 Vulnerability Management Standards 4200 - 4299 Vulnerability Management Procedures 4300 - 4399 Vulnerability Management Documents 4400 - 4499 Vulnerability Management Guidelines
5000 **Acceptable Use Policy**	5100 - 5199 Acceptable Use Standards 5200 - 5299 Acceptable Use Procedures 5300 - 5399 Acceptable Use Documents 5400 - 5499 Acceptable Use Guidelines
6000 **Security Awareness Policy**	6100 - 6199 Security Awareness Standards 6200 - 6299 Security Awareness Procedures 6300 - 6399 Security Awareness Documents 6400 - 6499 Security Awareness Guidelines
7000 **Risk Management Policy**	7100 - 7199 Risk Management Standards 7200 - 7299 Risk Management Procedures 7300 - 7399 Risk Management Documents 7400 - 7499 Risk Management Guidelines

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

- **Policies -** Description of the overall framework within which DCSS and Applicable Organizations authorize, direct and implement information security.
- **Standards** –More detailed mandatory directives are described in standards. As with Policies, Standards describe roles and responsibilities for carrying out directives.
- **Procedures** – Procedures are descriptions of detailed step by step actions to be taken to carry out policy or standard directives. Procedures also describe roles and responsibilities for conducting procedure steps.
- **Documents** – Documents are used to support policy and standards and procedures. Documents include forms, worksheets, logs, checklists, etc.
- **Guidelines** – Guidelines are descriptions of industry or Child Support Program best practices that are recommended but are not mandatory.

Section 3: Updating the Information Security Manual

Information Security Policies, Standards and Procedures that are formally adopted into the DCSS ISM will be enforced. Guidelines are not enforced, but are provided as a recommendation. Consequently, all proposed additions, updates, or deletions must go through an approval process before the DCSS ISM will be updated. The DCSS ISM is maintained by the DCSS CISO and the following process will be used for modifications to the DCSS ISM:

1. The DCSS CISO will update the DCSS ISM as necessary.
2. The requester will contact the DCSS CISO to discuss the suggested changes or additions.
3. If the suggestion is approved by the DCSS CISO, the requester will submit a draft of the Policy, Procedure, Standard, or Guideline to the DCSS CISO.
4. The DCSS CISO will work closely with the requester to refine the final draft and ensure consistency with existing DCSS ISM elements.
5. The DCSS CISO will present the draft to the Security Review Panel for review and approval.
6. If approved by the Security Review Panel, the draft will go to the DCSS Director for approval and subsequent inclusion into the DCSS ISM.

Please contact the DCSS Information Security Office (ISO), at (916) 464-5045, for any questions regarding this process.

Section 4: Compliance with the Information Security Manual

The ISM applies to all Information, Information Systems, Information Technology Assets, and business processes that are used in support of the CA 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 Information Security Manual is mandatory to ensure a consistent and strategic approach to protection information and assets.

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

In addition to the ISM, all CA Child Support Program organizations are required to evaluate their processes and systems and if necessary, implement additional protection mechanisms to adequately protect CA Child Support Program Information and Assets.

Recognizing that some business processes and/or technical environments will prevent full compliance with the ISM, the ISM includes an exception request process (ISM 1200) to approve and track necessary exceptions.

Section 5: Compliance Enforcement & Auditing

1. To certify compliance with the ISM, each applicable organization will annually submit an Information Security Manual Compliance Certification (ISM 1310) by October 31 of each year.
2. Compliance with the ISM will be verified during reviews conducted by the DCSS Security Audits Unit.
3. Exceptions to the Information Security Manual will be considered only when the requested exception is documented using the DCSS ISM 1200 Exception Handling Procedure and submitted to the DCSS CISO.

THIS PAGE IS INTENTIONALLY LEFT BLANK

Department of Child Support Services

INFORMATION SECURITY MANUAL	NUMBER:	1200
Subject: Exception Handling Procedure	REVISED DATE:	Original

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 DCSS 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, Reporting

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

Section 4: References

State Administrative Manual Section 4841.2

1300 – Exception Request Form

Section 5: Control and Maintenance

Policy Version: 1.0

Date: TBD

Owner: DCSS Information Security Office

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

Policy Version: 1.0

Date: TBD

Owner: DCSS Information Security Office

Department of Child Support Services

INFORMATION SECURITY MANUAL	**NUMBER:**	**2000**
Subject: Asset Protection Policy	**REVISED DATE:**	**Original**

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 & 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 the DCSS ISM 2103 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 the DCSS ISM 3200 Security Incident Management Procedure.

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:

- Adhere to DCSS Security Policies, Standards and Procedures.
- 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 4841.5.
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 the DCSS ISM 2103 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, Reporting

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

Section 5: References

State Administrative Manual Section 4841.5

2100 - Access Control Standard

2101 – Password Standard

2102 – Remote Access Standard

2103 – Information and IT Asset Classification Standard

2104 - Mobile Computing Device Standard

2107 - Conflict Reccusal Standard

Section 6: Control and Maintenance

Policy Version: 1.0

Date: TBD

Owner: DCSS Information Security Office

Department of Child Support Services

INFORMATION SECURITY MANUAL	NUMBER:	2100
Subject: Access Control Standard	**REVISED DATE:**	**Original**

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 DCSS ISM 6000 Security Awareness Policy.

2.2.2 System Requirements

Any system that processes or stores Child Support Information will:

1. Meet the DCSS 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]
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.

[1] Automated Systems for Child Support Enforcement: A Guide for States, August 2000, Requirement H-2e

[2] Ibid, requirement H-4b

[3] Ibid, requirement H-4a

[4] Ibid, requirement H-2j

[5] Ibid, requirement H-2i

[6] Ibid, requirement H-3g

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

All Applicable Organizations will provide warnings on the system's logon banners informing Child Support Employees of conditions of use. The banner message will be placed at the user authentication point for every computer system containing 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. At a minimum, banner messages shall contain the following:

1. Notification to the Child Support Employee that they are accessing confidential information such as from the Internal Revenue Service, California Franchise Tax Board, California State Board of Equalization, California Employment Development Department and other Child Support Information.
2. The computer is for authorized users and for business related functions only.
3. Unauthorized use of the computer system is prohibited by federal law including 26 United States Code sections 7213(a), 7213A, and 7431.
4. Unauthorized use of the computer system is prohibited by California law including but not limited to California Penal Code section 502, and California Family Code section 17212.
5. Use of the computer system may be monitored.
6. Evidence of unauthorized use collected during monitoring may be used for adverse action or criminal prosecution of the user.
7. Logging on to the computer system indicates acceptance of the terms and conditions listed in the banner.

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.
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.

2.3.4 Inactivity Timeout and Restricted Connection Times

Any system that processes or stores Child Support Information will:

1. Automatically lock workstations after 15 minutes of inactivity.
2. Restrict connection times for applications or systems in accordance with the sensitivity as defined in DCSS ISM 2103 Information and IT Asset Classification Standard.

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. [8]

[7] Ibid, requirement H-2b

[8] Ibid, requirement H-2d

2.5 Monitoring-System Access and Use

Refer DCSS ISM 2105 Secure System Standard,

Section 3: Enforcement, Auditing, Reporting

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

Section 4: References

State Administrative Manual Section 4841.5

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

2000 – Asset Protection Policy

2101 – Password Standard

2102 – Remote Access Standard

2103 – Information and IT Asset Classification Standard

Section 5: Control and Maintenance

Policy Version: 1.0

Date: TBD

Owner: DCSS Information Security Office

Department of Child Support Services

INFORMATION SECURITY MANUAL	**NUMBER:**	**2101**
Subject: Password Standard	**REVISED DATE:**	**Original**

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 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.

[1] ACF Requirement H-2c

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 where they cannot be personally secured or store a password in an unencrypted electronic data file.
12. Not send password in an unencrypted e-mail or other non secure form of communication. When distributing account information to the requestor, the username and password should be sent in separate email messages or using 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 1200 Exception Handling Procedure and submitted to the DCSS CISO.
4. Any person may, at any time, anonymously report policy violations by telephone at (916) 464-5045 or by email to Info.Security@dcss.ca.gov.

Section 4: References

State Administrative Manual Section 4841.5

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

2000 – Asset Protection Policy

2100 – Access Control Standard

Section 5: Control and Maintenance

Policy Version: 1.0

Date: TBD

Owner: DCSS Information Security Office

Department of Child Support Services

INFORMATION SECURITY MANUAL	**NUMBER:**	**2102**
Subject: Remote Access Standard	**REVISED DATE:**	**07/02/2007**

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 the DCSS ISM 2104 Mobile Computing Device Standard.
3. Remote Access equipment must comply with the DCSS ISM 2111 Encryption Standard.
4. Remote Access using wireless connections must comply with the DCSS 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, Reporting

1. Violation of this policy may result in disciplinary action that may include termination for employees and temporaries; termination of employment relations in the case of contractors or consultants; or dismissal for student assistants. Additionally, individuals may be subject to loss of Child Support Information access privileges, and if warranted, civil, or criminal prosecution under California or federal law.

2. DCSS is responsible for the periodic auditing and reporting of compliance with this policy. DCSS will define the format and frequency of the reporting requirements and communicate those requirements, in writing, to Applicable Organizations. In addition, DCSS Management can conduct an ad hoc audit at any time.

3. Exceptions to this policy will be considered only when the requested exception is documented using the DCSS ISM 1200 Exception Handling Procedure and submitted to the DCSS CISO.

4. Any person may, at any time, anonymously report policy violations by telephone at (916) 464-5045 or by email to Info.Security@dcss.ca.gov.

Section 4: References

State Administrative Manual Section 4840

1200 – Exception Handling Process

1300 – Exception Request Form

2000 – Asset Protection Policy

2100 – Access Control Standard

2101 – Password Standard

2104 – Mobile Computing Device Standard

2111 – Encryption Standard

2114 – Wireless Remote Communication Standard

Section 5: Control and Maintenance

Policy Version: 1.0

Date: TBD

Owner: DCSS Information Security Office

Department of Child Support Services

INFORMATION SECURITY MANUAL	**NUMBER:**	**2103**
Subject: Information and IT Asset Classification Standard	**REVISED DATE:**	**Original**

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 4841.3, 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 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.

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.

(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 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.

2.4 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.

Section 3: Enforcement, Auditing, Reporting

1. Violation of this policy may result in disciplinary action that may include termination for employees and temporaries; termination of employment relations in the case of contractors or consultants; or dismissal for student assistants. Additionally, individuals may be subject to loss of Child Support Information access privileges, and if warranted, civil, or criminal prosecution under California or federal law.
2. DCSS is responsible for the periodic auditing and reporting of compliance with this policy. DCSS will define the format and frequency of the reporting requirements and communicate those requirements, in writing, to Applicable Organizations. In addition, DCSS Management can conduct an ad hoc audit at any time.

3. Exceptions to this policy will be considered only when the requested exception is documented using the DCSS ISM 1200 Exception Handling Procedure and submitted to the DCSS CISO.

4. Any person may, at any time, anonymously report policy violations by telephone at (916) 464-5045 or by email to Info.Security@dcss.ca.gov.

Section 4: References

State Administrative Manual Section 4841.3

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

2000 – Asset Protection Policy

1200 – Exception Handling Process and Form

Section 5: Control and Maintenance

Policy Version: 1.0

Date: TBD

Owner: DCSS Information Security Office

Department of Child Support Services

INFORMATION SECURITY MANUAL	**NUMBER:**	**2104**
Subject: Mobile Computing Device Standard	**REVISED DATE:**	**Original**

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. Enforce lockout policy after 10 minutes of nonuse requiring reentering password to unlock.
5. For any MCD that will be used to store Child Support Information, install an encryption algorithm that meets or exceeds industry recommended encryption standard.
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 per DCSS ISM 3200 Security Incident Handling Procedure.

Section 3: Enforcement, Auditing, Reporting

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

Section 4: References

State Administrative Manual Section 4841.5

Department of Finance Budget Letter 05-32: Encryption on Portable Devices

2000 – Asset Protection Policy

Section 5: Control and Maintenance

Policy Version: 1.0

Date: TBD

Owner: DCSS Information Security Office

Department of Child Support Services

INFORMATION SECURITY MANUAL	NUMBER:	2105
Subject: Secure System Standard	REVISED DATE:	Original

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.

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

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

[2] Ibid, requirement H-3c

[3] Ibid, requirement H-4d

[4] Ibid, requirement H-4e

Violence Indicator, etc.) including identification of the responsible system user/caseworker and date/time of the change. [5]

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. [6]
3. The system must detect, record, and lock out unauthorized attempts to gain access to system software and data. [7]
4. The system must be capable of routinely monitoring the access to use of the automated system. [8]
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.[9]

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.

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.[10] Using copies of production data in a test environment is acceptable when necessary to adequately test the system.

Section 3: Enforcement, Auditing, Reporting

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

[5] Ibid, requirement H-2i

[6] Ibid, requirement H-3f

[7] Ibid, requirement H-2f

[8] Ibid, requirement H-2j

[9] Ibid, requirement H-3e

[10] Ibid, requirement H-3d

Section 4: References

State Administrative Manual Section 4841.5

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

1200 – Exception Handling Process and Form

2000 – Asset Protection Policy

Section 5: Control and Maintenance

Policy Version: 1.0

Date: TBD

Owner: DCSS Information Security Office

Department of Child Support Services

INFORMATION SECURITY MANUAL	**NUMBER:**	**2107**
SUBJECT: CONFLICT RECUSAL STANDARD	**REVISED DATE:**	**Original**

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 Child Support Information in any form 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, Reporting

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

Section 5: References

State Administrative Manual Section 4841.5

2000 – Asset Protection Policy

2100 – Access Control Standard

Section 6: Control and Maintenance

Policy Version: 1.0

Date: TBD

Owner: DCSS Information Security Office

Department of Child Support Services

INFORMATION SECURITY MANUAL	**NUMBER:**	**2111**
Subject: Encryption Standard	**REVISED DATE:**	**Original**

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 Section 4841.2, 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 DCSS 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 DCSS 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, Reporting

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

Section 4: References

State Administrative Manual Section 4841.2

State Administrative Manual Section 4841.3

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

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

2000 – Asset Protection Policy

2103 – Information and IT Asset Classification Standard

Section 5: Control and Maintenance

DCSS Policy will be reviewed and revised in accordance with parameters established in the Information Security Charter and Policy Management Process.

Department of Child Support Services

INFORMATION SECURITY MANUAL	NUMBER:	2114
Subject: Wireless Communication Standard	REVISED DATE:	Original

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 the DCSS 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 DCSS 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, 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 interns and volunteers. 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 can conduct an adhoc audit at any time.
3. Exceptions to this policy will be considered only when the requested exception is documented using the DCSS ISM 1200 Exception Handling Procedure and submitted to the DCSS Chief Information Security Officer.
4. Any person may, at any time, anonymously report policy violations by telephone at (916) 464-5045 or by email to Info.Security@dcss.ca.gov.

Section 4: References

1200 – Exception Handling Procedure

1300 – Exception Request Form

2000 – Asset Protection Policy

2102 - Remote Access Standard

2111 - Encryption Standard

2113 – Network Security Standard (in progress)

Section 5: Control and Maintenance

DCSS Policy will be reviewed and revised in accordance with parameters established in the Information Security Charter and Policy Management Process.

Department of Child Support Services

INFORMATION SECURITY MANUAL	**NUMBER:**	**3000**
SUBJECT: THREAT MANAGEMENT POLICY	**REVISED DATE:**	**Original**

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 & 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: DCSS ISM 7000 Risk Management Policy and DCSS 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 per DCSS ISM 3100 Incident Handling 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 the DCSS 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 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 a DCSS ISM 3200 Incident Handling Procedures to facilitate reporting of security incidents by all Applicable Organizations' Management.
5. Applicable Organizations' Management will report security incidents per the DCSS Incident Handing Procedure, DCSS ISM 3200 Incident Handling Procedures.
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, Reporting

1. Violation of this policy may result in disciplinary action that may include termination for employees and temporaries; termination of employment relations in the case of contractors or consultants; or dismissal for student assistants. Additionally, individuals may be subject to loss of Child Support Information access privileges, and if warranted, civil, or criminal prosecution under California or federal law.

2. DCSS is responsible for the periodic auditing and reporting of compliance with this policy. DCSS will define the format and frequency of the reporting requirements and communicate those requirements, in writing, to Applicable Organizations. In addition, DCSS Management can conduct an ad hoc audit at any time.
3. Exceptions to this policy will be considered only when the requested exception is documented using the DCSS ISM 1200 Exception Handling Procedure and submitted to the DCSS CISO.
4. Any person may, at any time, anonymously report policy violations by telephone at (916) 464-5045 or by email to Info.Security@dcss.ca.gov.

Section 5: References

State Administrative Manual Section 4845 - Incident Reporting

DCSS ISM 3100 Security Incident Standard

DCSS ISM 3200 Security Incident Handling Procedure

DCSS ISM 3300 Security Incident Reporting Form

Section 6: Section 6 - Control and Maintenance

Policy Version: 1.0

Date: TBD

Owner: DCSS Information Security Office

Department of Child Support Services

INFORMATION SECURITY MANUAL	NUMBER:	3100
Subject: Security Incident Management Standard	REVISED DATE:	07/02/2007

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.

For the purpose of this standard a security incident is 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.

This Security Incident Management Standard provides: 1) guidance and consistency for handling information security incidents by establishing DCSS incident management, monitoring and communication protocols; 2) directs all Applicable Organizations to establish and maintain effective incident handling procedures; 3) describes incident reporting requirements and procedures for Applicable Organizations.

This standard has the following sections:

- Establishing and Maintaining Procedures
- Incident Reporting Requirements

Section 2: Standard Directives

2.1 Establishing and Maintaining 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 twenty four hours a day, seven days per week.
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. Documentation of incidents during and at the completion of incident resolution.

2.2 Incident Reporting Requirements

All Applicable Organizations and DCSS employees must report security incidents to the DCSS Security Desk as specified below:

2.2.1 Incidents that must be reported to the DCSS Security Desk

1. DCSS employees and contractors are required to report all security incidents to the DCSS Security Desk as soon as practical, but no later than 1 hour after the event is detected.
2. Employees and contractors of Applicable Organizations must report to the DCSS Security Desk as soon as practical, but no later than 2 hours after the event is detected**, security incidents that involve:**
   - Child Support Information or Child Support IT Assets and
   - one of the following situations
     a. State-owned or State managed data (including Child Support data), has been damaged, destroyed, lost, stolen, deleted, shared, altered, copied, or used for non-Child Support business without authorization. This includes computer documentation and configuration information, as well as electronic and non-electronic data and reports.
     b. Unauthorized parties accessed one or more computers, computer systems or computer networks that store or process Child Support Information.
     c. Someone has accessed and without permission added, altered, damaged, deleted, or destroyed any computer software or computer programs which reside or exist internal or external to a computer, computer system, or computer network that contains or which provides access to Child Support Information Assets.
     d. Disruption of or denial of Child Support computer services occurs in a manner that appears to have been caused by deliberate and unauthorized acts.
     e. A contaminant has infected any computer, computer system, or computer network that contains or which provides access to Child Support Information Assets. This includes, but is not limited to viruses, Trojans, worms, and other types of malicious attacks.
     f. Internet domain names and/or user account names have been used without permission in connection with the sending of one or more electronic mail messages, and thereby caused damage to a computer, computer system, or computer network that contains or which provides access to Child Support Information Assets.
     g. Internet domain names and/or user account names have been used without permission in connection with the sending of one or more electronic mail messages which included misrepresentations regarding the Child Support Program or Child Support Information Assets.
     h. Damage or destruction of information processing facilities has occurred that may affect the integrity, availability or access to Child Support Information Assets.
     i. A physical intrusion into the facility of an Applicable Organization has occurred that may have resulted in compromise of Child Support Information Assets.

2.2.2 How to Report a Security Incident

Follow instructions in the DCSS ISM 3500 DCSS Security Incident Report Form available on the DCSS website.

Security incidents may be reported by any of the following methods:

1. Call the DCSS Security Desk at 888-DCSS-HELP (888-327-7435).
2. Email the DCSS Security Desk at Info.Security@DCSS.CA.GOV.
3. Hand deliver a written report to the DCSS Security guard station at 11120 International Drive, Rancho Cordova, CA.

4. Mail a written report to:

    Department of Child Support Services
    P.O. Box 419064
    Rancho Cordova, CA 95741-9064
    Attention: Information Security Office, Mail Stop 10

Section 3: Enforcement, Auditing, Reporting

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

Section 4: References

3000 -Threat Management Policy

Section 5: Control and Maintenance

Policy Version: 1.0

Date: TBD

Owner: DCSS Information Security Office

Department of Child Support Services Standard

INFORMATION SECURITY MANUAL	NUMBER:	3101
SUBJECT: DISASTER RECOVERY STANDARD	REVISED DATE:	Original

Section 1: Introduction

State Administrative Manual Section 4842.3 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]

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.

[1] Automated Systems for Child Support Enforcement: A Guide for States, August 2000, requirement H-5a

[2] Ibid, requirement H-5d

[3] Ibid, requirement H-5e

[4] Ibid, requirement H-5b

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, Reporting

1. Violation of this policy may result in disciplinary action that may include termination for employees and temporaries; termination of employment relations in the case of contractors or consultants; or dismissal for student assistants. Additionally, individuals may be subject to loss of Child Support Information access privileges, and if warranted, civil, or criminal prosecution under California or federal law.

2. DCSS is responsible for the periodic auditing and reporting of compliance with this policy. DCSS will define the format and frequency of the reporting requirements and communicate those requirements, in writing, to Applicable Organizations. In addition, DCSS Management can conduct an ad hoc audit at any time.

3. Exceptions to this policy will be considered only when the requested exception is documented using the DCSS ISM 1200 Exception Handling Procedure and submitted to the DCSS CISO.

4. Any person may, at any time, anonymously report policy violations by telephone at (916) 464-5045 or by email to Info.Security@dcss.ca.gov.

Section 4: References

State Administrative Manual, Sect 4843

2000 Asset Protection Policy

3000 Threat Management Policy

1200 Exception Handling Process and Form

U.S. Department of Health and Human Services/ ACF, Automated System for Child Support Enforcement: A Guide for States, August 2000; ACF-H5

Section 5: Control and Maintenance

Policy Version: 1.0

Date: TBD

Owner: DCSS Information Security Office

Department of Child Support Services

INFORMATION SECURITY MANUAL	**NUMBER:**	**3102**
Subject: Virus Management Standard	**REVISED DATE**	**Original**

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 the DCSS 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 DCSS ISM 3300 Incident Reporting Form.

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 interns and volunteers. 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 can conduct an adhoc audit at any time.
3. Exceptions to this policy will be considered only when the requested exception is documented using the DCSS ISM 1200 Exception Handling Procedure and submitted to the DCSS Chief Information Security Officer.

4. Any person may, at any time, anonymously report policy violations by telephone at (916) 464-5045 or by email to Info.Security@dcss.ca.gov.

Section 4: References

1200 – Exception Handling Process and Form

2000 – Asset Protection Policy

3000 - Threat Management Policy

3100 – Security Incident Management Standard

Section 5: Control and Maintenance

DCSS Policy will be reviewed and revised in accordance with parameters established in the Information Security Charter and Policy Management Process.

Department of Child Support Services

INFORMATION SECURITY MANUAL	**NUMBER:**	**4000**
Subject: Vulnerability Management Policy	**REVISED DATE:**	**Original**

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 & 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 the DCSS ISM 3200 Security Incident Handling Procedure 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 1200 Exception Handling Procedure and submitted to the DCSS CISO.
4. Any person may, at any time, anonymously report policy violations by telephone at (916) 464-5045 or by email to Info.Security@dcss.ca.gov.
5.

Section 5: References

State Administrative Manual Section 4840

ISM 4100 Configuration Management Standard

Section 6: Control and Maintenance

Policy Version: 1.0

Date: TBD

Owner: DCSS Information Security Office

Department of Child Support Services

INFORMATION SECURITY MANUAL	**NUMBER:**	**4100**
SUBJECT: CONFIGURATION MANAGEMENT STANDARD	**REVISED DATE:**	**Original**

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.
4. A Configuration Management Log must be maintained for all changes.

[1] U.S. Department of Health and Human Services/ ACF, Automated System for Child Support Enforcement: A Guide for States, August 2000, requirement H-3a

[2] Ibid, requirement H-3b

5. All configuration changes must be tested in the test environment prior to implementing into production.

Section 3: Enforcement, Auditing, Reporting

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

Section 4: References

State Administrative Manual Section 4841.5

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

4000 – Vulnerability Management Policy

Section 5: Control and Maintenance

Policy Version: 1.0

Date: TBD

Owner: DCSS Information Security Office

Department of Child Support Services

INFORMATION SECURITY MANUAL	NUMBER:	4101
Subject: Patch Management Standard	REVISED DATE:	Original

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:

1. A method to determine in a timely manner, the existing patch levels for all firmware and software used by the applicable organization.
2. A requirement that all patches must be obtained from authorized sources or supported vendors.
3. A documented change management process to ensure patches are approved and implemented in a controlled fashion.
4. 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, Reporting

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 interns and volunteers. 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.

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 can conduct an adhoc audit at any time.

Exceptions to this policy will be considered only when the requested exception is documented using the DCSS ISM 1200 Exception Handling Procedure and submitted to the DCSS Chief Information Security Officer.

Any person may, at any time, anonymously report policy violations by telephone at (916) 464-5045 or by email to Info.Security@dcss.ca.gov.

Section 4: References

1200 – Exception Handling Process and Form

2000 – Asset Protection Policy

DCSS ISM 4000 Vulnerability Management Policy

Section 5: Control and Maintenance

DCSS Policy will be reviewed and revised in accordance with parameters established in the Information Security Charter and Policy Management Process.

Department of Child Support Services

INFORMATION SECURITY MANUAL	**NUMBER:**	**5000**
Subject: Acceptable Use Policy	**REVISED DATE:**	**Original**

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 & 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 using the DCSS ISM 3200 Incident Handling Procedures.
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.

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, Reporting

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

Section 5: References

Government Code Section 8314

Section 6: Control and Maintenance

Policy Version: 1.0

Date: TBD

Owner: DCSS Information Security Office

Department of Child Support Services

INFORMATION SECURITY MANUAL	**NUMBER:**	**6000**
Subject: Security Awareness Policy	**REVISED DATE:**	**Original**

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 & 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, Standards and Procedures.

Section 4: Enforcement, Auditing, Reporting

1. Violation of this policy may result in disciplinary action that may include termination for employees and temporaries; termination of employment relations in the case of contractors or consultants; or dismissal for student assistants. Additionally, individuals may be subject to loss of Child Support Information access privileges, and if warranted, civil, or criminal prosecution under California or federal law.

2. DCSS is responsible for the periodic auditing and reporting of compliance with this policy. DCSS will define the format and frequency of the reporting requirements and communicate those requirements, in writing, to Applicable Organizations. In addition, DCSS Management can conduct an ad hoc audit at any time.
3. Exceptions to this policy will be considered only when the requested exception is documented using the DCSS ISM 1200 Exception Handling Procedure and submitted to the DCSS CISO.
4. Any person may, at any time, anonymously report policy violations by telephone at (916) 464-5045 or by email to Info.Security@dcss.ca.gov.

Section 5: References

State Administrative Manual Section 4840

Section 6: Control and Maintenance

Policy Version: 1.0

Date: TBD

Owner: DCSS Information Security Office

Department of Child Support Services

INFORMATION SECURITY MANUAL	**NUMBER:**	**7000**
Subject: Risk Management Policy	**REVISED DATE:**	**Original**

Section 1: Introduction

Risk is the net negative impact of the exercise of a 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 & 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. Exceptions to this policy will be considered only when the requested exception is documented using the DCSS ISM 1200 Exception Request Procedure and submitted to the DCSS Chief Information Security Officer.

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 Risk Management Plan 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 the DCSS ISM 3200 Incident Handling Procedures. 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.
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, 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.

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

[2] ACF Requirement H-1

3. Exceptions to this policy will be considered only when the requested exception is documented using the DCSS ISM 1200 Exception Handling Procedure and submitted to the DCSS CISO.

4. Any person may, at any time, anonymously report policy violations by telephone at (916) 464-5045 or by email to Info.Security@dcss.ca.gov.

Section 5: References

State Administrative Manual Section 4840

4100 - Configuration Management Standard

Section 6: Control and Maintenance

Policy Version: 1.0

Date: TBD

Owner: DCSS Information Security Office

Appendices

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
PO 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 Number	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

INFORMATION SECURITY EXCEPTION REQUEST

3. Scope of requested exception(s): Organizational unit to which the exceptions(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 location(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)?

INFORMATION SECURITY EXCEPTION REQUEST

DCSS ISM 1300 (07/25/07)

What will be 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

INFORMATION SECURITY EXCEPTION REQUEST

DCSS ISM 1300 (07/25/07)

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 BRANCH

7. Approval/Rejection details.

Details of Approval/Rejection

Approval	Disapproval

Details

Conditions

Projected Review Date

STATE OF CALIFORNIA - HEALTH AND HUMAN SERVICES AGENCY　　DEPARTMENT OF CHILD SUPPORT SERVICES

ANNUAL INFORMATION SECURITY MANUAL COMPLIANCE CERTIFICATION

DCSS ISM 1310 (03/30/07)

In order to comply with the DCSS Information Security Manual, Section 1000, it is necessary to complete, sign, and return this form to the Department of Child Support Services by October 31st of each year. This form is to be completed by the Director or Director's designee.

Please return the completed, signed form to:

Department of Child Support Services
Attn: Information Security Office
PO Box 419064
Rancho Cordova, CA 95741-9064

Name of Agency/Organization	
Name of Information Security Officer	Phone Number/Email Address
Name of Additional Contact	Phone Number/Email Address

I certify that I am the Director or Director's designee and, as prescribed in the DCSS Information Security Manual, Section 1000 Introduction, I certify that this organization is in compliance with the following:

- DCSS Information Security Manual
- Ensuring annual training is conducted for all employees, contractors, and other individuals who have access to personal, confidential, or sensitive information and certifying their understanding of the consequences of violating information privacy and security policies by signing the DCSS Confidentiality Statement (DCSS 0593)
- Confidentiality Statements are signed and maintained for each new employee within 30 days of hire

Check one:

□ Our agency/organization is currently in compliance with the DCSS Informaton Security Manual or an Exception Request form (DCSS ISM 1300) has been submitted for all areas of noncompliance.

□ Our agency/organization will be in compliance with the DCSS Information Security Manual by (mm/dd/yyyy). Submit an Exception Request form for all areas of noncompliance and attach it to this form.

Signature of Director or Designee	Date

Department of Child Support Services
Security Incident Report

To report a security incident, call the Security Desk at (916) 464-5045. Someone will assist you 24 hours per day. If you perceive immediate danger to yourself or to others, please call 911 immediately. And then call the Security Desk.

The attached form will assist you in reporting any incident that threatens:

- persons or property at any child support facility; or
- confidentiality, integrity, or availability of child support information

You may report an incident anonymously by completing the attached form and submitting it to email DCSSInformationSecurityOffice@DCSS.CA.GOV or delivering a hard copy to the DCSS Guard Station at 11120 International Drive, Rancho Cordova. However, you may also report an incident anonymously by calling the Security Desk and requesting that your report be treated anonymously.

If you are unsure whether the event or activity you have observed should be reported, call the Security Desk for assistance.

To report an incident, complete all Sections that apply below.

SECTION I – Reporter Information	
Your Name	
Your contact number	
Your email address	
Current date	

SECTION II INSTRUCTIONS: Complete Section II to report an incident that involves a threat or harm to persons or property

SECTION II – Persons/Property Incident Information			
Check all boxes that apply to incident.			
□ harassment	□ fire alarm	□ gang activity	□ burglary
□ personal threats of violence	□ loss of state equipment	□ theft	□ facility damage
□ robbery	□ theft of state property	□ graffiti	□ physical intrusion
□ weapons at facility	□ trespassing	□ bomb threat	□ other

SECTION III INSTRUCTIONS: Complete Section II to report an incident that involves harm or a threat to the confidentiality, integrity or availability of child support information

SECTION III – Information Security Incident Information			
Check all boxes that apply to incident.			
□ misuse of confidential or sensitive information	□ unauthorized destruction of information	□ fraudulent solicitation of child support information	□ email threats or harassment
□ misuse of state property	□ theft or loss of child support information	□ improper disposal of child support information	□ other threat to child support systems or information
□ unauthorized disclosure of personal information	□ unauthorized modification or deletion of data	□ unexplained system crashes	□ malicious software attack or infection (worms, viruses)
□ unauthorized changes in file permissions	□ attempts to write to system files or change systems files	□ abnormally slow or poor system performance	□ suspicious log discrepancies
□ unknown or suspicious files	□ modification, installation, or deletion of software	□ unauthorized installation or use of program	□ unauthorized use of network scanners, sniffers, or other traffic capturing devices
□ system alarm	□ physical or logical damage to a system	□ denial of service attack	□ embezzlement or fraud
□ user accounts not created by system administrators	□ unauthorized local or remote access	□ modifications to file lengths or dates	□ unusual logon attempts

Go on to Next Page to Provide Details of Incident

Official Use

SECTION IV INSTRUCTIONS: Complete for all incidents

SECTION IV

Complete all information that applies

Date you observed the incident	Time you observed the incident

Physical location of incident (examples: address or name of facility including floor, room, cube, coordinates, etc.):

System or Network affected (examples: email, network, time reporting, webpage, etc.):

Identify all Organizations you have contacted regarding this incident. Check all incidents that apply.

□ CHP	□ DCSS Business Services	□ Others (Specify)
□ Local police	□ SDU Security Officer	
□ 9-1-1	□ LCSA (or county) Security Office	

SECTION V INSTRUCTIONS: Complete for all incidents

SECTION V – Details of Incident

Describe the incident.

Official Use

Go on to Next Page to Provide Information Regarding Persons with Information

SECTION VI INSTRUCTIONS: Complete for all incidents

SECTION VI – Persons with Information

Identify other persons involved in the incident. A Victim is anyone who is threatened or harmed by the incident. A Witness is anyone that you believe may have information that may assist in the investigation of the incident

□ Victim	□ Witness	Name
		Contact Information
□ Victim	□ Witness	Name
		Contact Information
□ Victim	□ Witness	Name
		Contact Information
□ Victim	□ Witness	Name
		Contact Information

Official Use