

CALIFORNIA DEPARTMENT OF CHILD SUPPORT SERVICES

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



May 5, 2010

CSS LETTER: 10-05

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

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

SUBJECT: NEW INFORMATION SECURITY STANDARDS AND REVISIONS TO THE INFORMATION SECURITY MANUAL (SUPERSEDES AND REPLACES CSS LETTER 04-10)

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

The revisions to existing ISM policies and standards are outlined in the attached ISM Record of Changes. The new standards and guideline, attached, are listed below.

- 2110 Media Protection and Sanitation Standard
- 2112 Systems Acquisition, Development and Maintenance Standard
- G-01-01 Media Sanitation Guideline

ISM 2110 Media Protection and Sanitation Standard together with the accompanying guideline supersede CSS Letter 04-10. The ISM and supporting guidelines and forms are available online from the Information Security link on the California Child Support Central website <https://central.dcss.ca.gov/Pages/Default.aspx>.

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

Sincerely,

MARY ANN MILLER
Assistant Director, Office of Executive Programs

Attachments: ISM Record of Changes
ISM 2110 Media Protection and Sanitation
ISM 2112 Systems Acquisition, Development and Maintenance
G-10-01 Media Sanitation



Information Security Manual

Record of Changes

May 2010

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

THIS PAGE IS INTENTIONALLY LEFT BLANK



Department of Child Support Services

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

Section 1: Introduction

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

Standard directives include the following:

- Media Access and Storage
- Media Sanitation

Section 2: Standard Directives

2.1 Media Access and Storage

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

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

INFORMATION SECURITY MANUAL		NUMBER:	2110
Subject:	Media Protection and Sanitation		Page 2 of 4

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

2.2 Media Sanitation

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

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

INFORMATION SECURITY MANUAL		NUMBER:	2110
Subject:	Media Protection and Sanitation		Page 3 of 4

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

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

Section 3: Enforcement, Auditing, and Reporting

1. Violation of this policy may result in disciplinary action that may include termination for employees and temporaries; termination of employment relations in the case of contractors or consultants; or dismissal for student assistants. Additionally, individuals may be subject to loss of Child Support Information access privileges, and if warranted, civil, or criminal prosecution under California or federal law.
2. DCSS ISO is responsible for the periodic auditing and reporting of compliance with this policy. DCSS will define the format and frequency of the reporting requirements and communicate those requirements, in writing, to Applicable Organizations. In addition, DCSS ISO can conduct an ad hoc audit at any time.
3. Exceptions to this policy will be considered only when the requested exception is documented using the DCSS ISM 1300 Information Security Exception Request Form and submitted to the DCSS CISO.
4. Any person may, at any time, anonymously report policy violations by telephone at (916) 464-5045 or by email to Info.Security@dcss.ca.gov.

Section 4: Related Policies and Standards

ISM 2103 – Information and IT Asset Classification Standard

ISM 2108 – Physical Security Standard

ISM 2111 – Encryption Standard

INFORMATION SECURITY MANUAL		NUMBER:	2110
Subject:	Media Protection and Sanitation		Page 4 of 4

Section 5: References

SAM Section 5320 – Asset Protection

SAM Section 5345.2 – Cryptography

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

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

NIST SP 800-88 – Guidelines for Media Sanitization

Section 6: Control and Maintenance

Issued: May 1, 2010

Owner: DCSS Information Security Office



Department of Child Support Services

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

Section 1: Introduction

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

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

Section 2: Standard Directives

2.1 IT Security Capital Planning

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

2.2 System Development Life Cycle Requirements

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

2.2.1 Initiation

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

INFORMATION SECURITY MANUAL	NUMBER:	2112
Subject: SYSTEMS ACQUISITION, DEVELOPMENT, AND MAINTENANCE		Page 2 of 5

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

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

2.2.2 Development and Acquisition

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

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

2.2.3 Implementation and Assessment

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

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

INFORMATION SECURITY MANUAL	NUMBER:	2112
Subject: SYSTEMS ACQUISITION, DEVELOPMENT, AND MAINTENANCE		Page 3 of 5

2.2.4 Operations and Maintenance

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

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

2.2.5 Disposal

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

INFORMATION SECURITY MANUAL	NUMBER:	2112
Subject: SYSTEMS ACQUISITION, DEVELOPMENT, AND MAINTENANCE		Page 4 of 5

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

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

Section 3: Enforcement, Auditing, and Reporting

1. Violation of this policy may result in disciplinary action that may include termination for employees and temporaries; termination of employment relations in the case of contractors or consultants; or dismissal for student assistants. Additionally, individuals may be subject to loss of Child Support Information access privileges, and if warranted, civil, or criminal prosecution under California or federal law.
2. DCSS is responsible for the periodic auditing and reporting of compliance with this policy. DCSS will define the format and frequency of the reporting requirements and communicate those requirements, in writing, to Applicable Organizations. In addition, DCSS management can conduct an ad hoc audit at any time.
3. Exceptions to this policy will be considered only when the requested exception is documented using the DCSS ISM 1300 Information Security Exception Request Form and submitted to the DCSS CISO.
4. Any person may, at any time, anonymously report policy violations by telephone at (916) 464-5045 or by email to Info.Security@dcss.ca.gov.

Section 4: Related Policies and Standards

ISM 2105 – Secure System Standard

ISM 2103 – Information and IT Asset Classification

ISM S-10-01 – Media Protection and Handling

Section 5: References

SAM Section 4904 – Information Technology Five-Year Capital Plan

SAM Section 5320.5 – Classification of Information

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

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

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

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

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

INFORMATION SECURITY MANUAL	NUMBER:	2112
Subject: SYSTEMS ACQUISITION, DEVELOPMENT, AND MAINTENANCE		Page 5 of 5

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

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

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

Section 6: Control and Maintenance

Owner: DCSS Information Security Office

Issued: May 1, 2010



Department of Child Support Services

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

1.0 Purpose

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

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

2.0 Sanitation Methods

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

Table 1

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

INFORMATION SECURITY MANUAL		NUMBER:	G-10-01
Subject:	Media Sanitization Guideline		Page 2 of 5

Method	Description	Examples
	information against laboratory attack, which is data scavenging or retrieval through laboratory means. This typically involves the use of signal processing equipment and specially trained personnel. Executing the secure erase firmware command on a disk is an acceptable method of purging.	Erase Utility http://cmrr.ucsd.edu/people/Hughes/SecureErase.shtml Note: Tapes are capable of being purged for re-use with the use of degaussers. Degaussing hard drives typically renders the drive useless. Refer to "Degaussers" under the Destroying method of this table.
Destroying	The ultimate form of sanitation is to physically destroy the media. Physical destruction can be accomplished using a variety of methods with the objective of making the data unrecoverable or unable to be reconstructed. Optical media (e.g., CDs, DVDs) must be destroyed by pulverizing, shredding or incineration. <u>Use of a certified degausser is also an acceptable method of destroying electronic media.</u> Degaussing is not effective for optical media (e.g., CDs, DVDs).	For hard drives, any method of disrupting the full revolution of the hard drive platter is acceptable. Examples include drilling through hard drive platter, grinding platter with a sand grinder, hammering railroad spike through platter, etc. Optical mass storage media, including compact disks (CD, CD-RW, CD-R, and CD-ROM), optical disks (DVD), and magneto-optic (MO) disks should be destroyed by pulverizing, cross-cut shredding, or burning. Paper shredders can be used to destroy flexible media such as diskettes once the media are physically removed from their outer containers. The shred size of the refuse should be small enough that there is reasonable assurance that the information cannot be reconstructed. Degaussers: See approved list of degaussers evaluated and provided by the National Security Agency (NSA) in the document "Evaluated Products List - Degausses" dated March 2009." The degausser must be able to produce at least 5000 oersteds to be able to erase both Longitudinal and Perpendicular storage devices manufactured after year 2004. http://www.nsa.gov/ia/files/government/MDG/EPL-Degausser30March2009.pdf Shredders: See approved list of shredders evaluated and provided by NSA in the document "Evaluated Products List – High Security Crosscut Paper Shredders" dated April 2009." http://www.nsa.gov/ia/files/government/MDG/NSA_CSS-EPL-02-01.pdf IRS P1075 requires paper shredded to effect 5/16" wide or smaller strips; microfilm and microfiche shredded to

INFORMATION SECURITY MANUAL		NUMBER:	G-10-01
Subject:	Media Sanitization Guideline		Page 3 of 5

Method	Description	Examples
		effect a 1/35- inch by 3/8- inch strips. If shredding is part of the overall destruction of FTI, strips can in effect be set at the industry standard (currently 1/2"). However, when deviating from 5/16", FTI in this condition (i.e., strips larger than 5/16"), must be safeguarded until it reaches the stage where it is rendered unreadable.

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

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

Table 2

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

INFORMATION SECURITY MANUAL		NUMBER:	G-10-01
Subject:	Media Sanitization Guideline		Page 4 of 5

Media Type	Clear	Purge	Destroy
CDs/DVDs	N/A	N/A	Optical disk grinding device, incinerate, shred.
Paper and microfilms	N/A	N/A	Incinerate or shred

3.0 Sanitation Requirements

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

Table 3

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

Vendor Repairs

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

Certification of Sanitation

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

INFORMATION SECURITY MANUAL		NUMBER:	G-10-01
Subject:	Media Sanitization Guideline		Page 5 of 5

4.0 Related Policies and Standards

Media Protection and Sanitation Standard – ISM 2110

NIST SP 800-88 – Media Sanitation Guideline

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

NSA/CSS Media Destruction Evaluated Product Lists

5.0 References

California Civil Code Section 1798 (Information Practices Act)

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