STATE OF FLORIDA
DEPARTMENT OF
CHILDREN AND FAMILIES
TALLAHASSEE, October 6, 2022

CF OPERATING PROCEDURE
NO. 50-28

Systems Management

MEDIA PROTECTION

1. Purpose. This operating procedure provides the minimum security requirements for media protection to prevent the loss of confidentiality, integrity, or availability of the Department of Children and Families (Department or DCF) information stored on computer equipment or media.

a. As part of a defense-in-depth strategy, the Department routinely encrypts DCF data and information at rest on removable storage devices and portable media.

b. The Department uses cryptographic mechanisms techniques to ensure the maintenance of confidentiality and integrity of the information.

2. Scope. This operating procedure covers procedures for all computer equipment or media devices containing Department information, including that held by third parties on behalf of the Department.

a. Any information not explicitly identified as the property of other parties transmitted or stored on DCF information technology resources (including email messages and files) is the property of the Department.

b. All information technology resource users (DCF employees, contractors, vendors, or others) are responsible for adhering to this operating procedure.

c. As a part of the agency review process, all affiliated contractors who receive, transmit, process, or store confidential information/data on behalf of the Department are subject to review.

3. References.

a. Section 282.318, Florida Statutes, “State Cybersecurity Act.”

b. Section 501.171, Florida Statutes, “Security of Confidential Personal Information.”

c. Chapter 815, Florida Statutes, “Florida Computer Crimes Act.”

d. Chapter 60GG-2, Florida Administrative Code, “*Florida Cybersecurity Standards*.”

e. Internal Revenue Service (IRS), Publication 1075, “Safeguards Program.”

f. Title XIII, Section 13402, “Notification in the Case of Breach.”

g. 45 CFR Parts 160 and 164, Subparts A and C, “Health Information Portability and Accountability Act (HIPAA) Privacy and Security Rules.”

h. 26 U.S. Code § 6103, “Confidentiality and disclosure of returns and return information.”

i. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 5, “Security and Privacy Controls for Information Systems and Organizations.”

j. NIST SP 800-88 r1, “Guidelines for Media Sanitization.”

4. Definitions. For this operating procedure, the following terms shall apply:

a. Confidential Information/Confidential Data. Information not subject to inspection by the public that may be released only to those persons and entities designated in Florida statute; information designated as confidential under provisions of federal law or rule, including but not limited to: Federal Tax Information (FTI), Health Insurance Portability and Accountability Act (HIPAA) Protected Health Information (PHI), Personally Identifiable Information (PII), Social Security Numbers (SSN), and drivers’ license information and/or photographs.

b. Data Loss Prevention (DLP). Technical software-based strategy for ensuring end users do not send sensitive or critical information outside the DCF network by helping network administrators control what data end users can transfer.

c. Data Sanitization. A method by which a data destruction program overwrites the data on a hard drive or other storage devices, erasing confidential data, files, and records permanently.

d. Digital Media. May include diskettes, magnetic tapes, external/removable hard disk drives, flash drives, compact disks, and digital video disks.

e. Employee. Any person employed by the Department in an established position in the Senior Management Service, Selected Exempt Service, Career Service, or paid from Other Personal Services (OPS) funds. Also, for this operating procedure, the definition of employee includes any non-OPS temporary staff hired by the Department who have access to DCF IT resources, including contracted staff and contractor vendor staff.

f. Exempt Information. Information DCF is not required to disclose under section 119.07(1), F.S., but the Department does not necessarily prohibit from disclosing in all circumstances.

g. Information Custodians. Agency information technology workers who maintain or administer information resources on behalf of information owners. A person or team that holds the day-to-day responsibility for information technology infrastructure resources (may also be referred to as Data Custodian). Responsibilities include ensuring equipment sanitization takes place as provided in this operating procedure per all the Department’s information handling procedures.

h. Information Owner. The business unit manager is ultimately responsible for collecting, maintaining, and disseminating specific information collection. Responsibilities include maintaining a reference list of their exempt and confidential and exempt information and associated applicable state and federal statutes and rules and maintaining Department data per applicable retention requirements.

i. Information Security Manager/Officer. A person designated by the Secretary of the Department to report to the Chief Information Officer (CIO) and administer DCF's information technology security program, serving as the process owner for all ongoing activities that provide appropriate access to and protect the confidentiality and integrity of information in compliance with Department and statewide policies and standards per section 282.318, F.S., and Chapter 60GG-2, F.A.C.

j. Information Technology Resources. Data processing hardware (including desktop computers, laptops, tablets, smartphones, and associated devices), software and services, supplies, personnel, facility resources, maintenance, training, or other related resources.

k. Media. Digital media, including, are not limited to USB drives, diskettes, magnetic tapes, external/removable hard disk drives, compact disks, and digital video disks.

l. Media Sanitization. One of the key elements in assuring confidentiality of information. The Department utilizes a process that renders access to target data on the media device infeasible for a given level of effort. Clear, Purge, and Destroy are actions the Department takes to sanitize media:

(1) Clear. Apply analytic techniques to sanitize data in all user-addressable storage locations to protect against simple non-invasive data recovery techniques. Typically applied through the standard Read and Write commands to the storage device, such as rewriting with a new value or using a menu option to reset the device to the factory state (where rewriting is not supported).

(2) Purge. Also referred to as “wiping.” Higher security level than clearing. Applies physical or logical techniques that render target data recovery infeasible using state-of-the-art laboratory techniques.

(3) Destroy. Applies physical or logical techniques that render target data recovery infeasible using state-of-the-art laboratory techniques. Physical destruction methods include but are not limited to disintegration, incineration, pulverization, melting, and shredding.

m. Mobile Device. Any non-stationary electronic device with a singular or multiple capabilities of recording, storing, or transmitting data, voice, video, or photo images. In addition, to but not limited to laptops, personal digital assistants, pocket personal computers, MP3 players, smartphones, and video cameras.

5. Media Access. The Department restricts employee access to media based upon the classification of the data the media contains per CFOP 50-27, Data Classification and Access Control.

a. All Department data and information, regardless of the format or medium of the record (e.g., electronic data/voice/video/image, microfilm), should be classified as Level 1 Restricted, Level 2 Confidential, and Level 3 Public.

b. The Data Classification process determines which DCF employee roles can access which level(s) of data within a DCF business system and/or program office.

c. The Department protects removable digital media by providing encryption so that only authorized persons can access DCF data and information.

6. Media Marking. The Department restricts access to media based upon the classification system of the media’s data per CFOP 50-27, Data Classification and Access Control. As part of data classification, business systems and program areas shall mark all information system media per CFOP 80-2, Property Management. The labeling and associated labeling metadata indicate distribution limits, handling caveats, and applicable security markings to help support access control.

a. A program area director may exempt some types of information system media from marking as long as the media remains within the controlled area of the program office. Program office written business procedures should reflect or reference this decision.

b. The Department must establish adequate controls to prevent disclosing FTI to other state agencies, tax or non-tax, or political subdivisions, such as cities or counties, for any purpose, including tax administration, absent explicit written IRS authority granted under IRC 6103(p)(2)(B).

7. Media Storage. The Department shall control and securely store all media within the program area and/or business system, keeping it safe from unauthorized access. DCF shall protect information

system removable media until the media are destroyed or sanitized using approved equipment, techniques, and procedures.

a. Physically controlling information system media includes conducting monthly, quarterly, or annual inventories, ensuring procedures are in place to allow individuals to check out and return media to the media library, and maintaining documented accountabilities for all stored media.

b. Controlled areas are areas where the Department provides sufficient physical and procedural safeguards to meet the requirements for protecting information and/or information systems. Secure storage includes a locked drawer, desk, or cabinet, or a controlled media library.

c. The Department restricts access to media based upon the classification of the data the media contains per CFOP 50-27, Data Classification and Access Control. The type of media storage security in place shall be commensurate with the security category and/or classification of the information residing on the media.

d. For media containing information determined by the Department and/or the State of Florida to be in the public domain, publicly releasable, or have limited or no adverse impact on the Department, State, or individuals if accessed by other than authorized personnel, fewer safeguards may be needed. In these situations, physical access controls provide adequate protection.

8. Media Transport. The Department protects and controls information system media during transport outside of controlled areas using appropriate program office defined security safeguards, maintains accountability for information system media during transport, documents activities associated with the transport of information system media, and restricts the activities related to the transportation of information system media to authorized personnel.

a. Information system media includes, for example, diskettes, magnetic tapes, external/removable hard disk drives, flash drives, compact disks, and digital video disks. Mobile devices with information storage capability (e.g., smartphones, tablets) may fit the definition of storage media within a respective program area.

b. Controlled areas are areas or spaces for which the Department provides sufficient physical and/or procedural safeguards to meet the requirements established for protecting information and/or information systems.

c. Physical and technical safeguards for media are commensurate with the data classification level established by CFOP 50-27 for the information residing on the media.

d. Safeguards to protect media during transport are not limited to but include locked containers and password-based cryptography. Cryptographic mechanisms can provide confidentiality and integrity protection depending upon the means used and should be consistent with the compliance requirements of the program area. DCF program areas retain the right to be more restrictive in their business procedures to ensure compliance.

e. Department end-users should store encrypted external hard drives owned by their program office area in a secure location per CFOP 50-3, Security Planning.

f. Activities associated with transport include the actual transport, related activities to the media’s release, and ensuring that media enters the appropriate transport processes. For the essential transport, authorized transport and courier personnel may include individuals from outside the Department (e.g., U.S. Postal Service or a commercial carrier or delivery service that provides a tracking service).

g. Maintaining accountability of media during transport includes, for example, restricting transport activities to authorized personnel and tracking and/or obtaining detailed records of transport activities as the media moves through the transportation system to prevent and detect loss, destruction, or tampering.

h. Program areas shall establish documentation requirements for activities associated with the transport of information system media per the data classification level of the media plus assessments of risk associated with the chosen transport methodology. Program areas have the flexibility to define different record-keeping methods for different types of media transport as part of their overall system of transport-related records.

i. Confidential Information/Confidential Data shall not be copied from the system unless there is a business need that requires the transfer of confidential information or data. When files contain identifiable information or data, the files must be encrypted to prevent unauthorized disclosure. DCF requires encryption of all removable media to prevent a compromise or breach of Department confidential information or data. Encrypted files shall not be readable from non-Department-owned machines. The Department shall monitor all confidential information or data removed from the system. Detailed logs of such actions will include the user's name and the copied data. The Department shall implement tools to monitor and log or encrypt such activities.

9. Media Sanitization. To ensure compliance with rules about the disposition of confidential information, OITS must ensure data sanitization completed before the disposal, surplus, reuse, or offsite repair of any information technology resource.

a. The Department must use sanitization techniques and procedures per applicable federal and Department standards and policies. Sanitization mechanisms should always display strength and integrity in the information's security level and data classification level.

b. If the media is being reallocated, care should be taken to ensure that residual data does not exist and therefore cannot be recovered or accessed by unauthorized users. At DCF, data sanitization involves following the methods detailed in Department of Defense (DoD) 5220.22-M, the National Industrial Security Program Operating Manual, and/or NIST SP 800-88 r1, Guidelines for Media Sanitization. These methods involve overwriting all data tracks a minimum of three times, depending on risk level.

(1) These methods apply to all information system media subject to disposal or reuse, whether or not the media is considered removable. Examples are not limited to but include media found in scanners, copiers, printers, computer workstations, network components, and mobile devices.

(2) The sanitization process must remove information from the media such that the data cannot be retrieved or reconstructed.

(3) Sanitization techniques, including clearing, purging, and destruction, prevent the disclosure of information to unauthorized individuals when such media is reused or released for disposal and/or destruction.

(4) The Department determines the appropriate sanitization methods recognizing that the destruction method is necessary when other methods fail to render media data unrecoverable.

(5) The Department shall use an approved documentation and data retention method per all applicable state and federal statutes.

(6) Only authorized personnel shall prepare information technology devices that have contained confidential information for disposal, surplus, reuse, or offsite repair. Authorized personnel shall document when, how, and the method used for data sanitization.

(7) Multi-Function Devices. The Department shall ensure the sanitization of all hard drives on all leased multi-function devices at the end of service. Whenever these devices go off-lease or are designated for surplus, General Services shall notify IT security staff. If DCF owns the hard drives as part of contracted services, the vendor will remove the hard drives, and DCF staff will store them in a secure onsite location until IT security staff take possession and sanitize or destroy the hard drives. When DCF opt not to own the hard drives on leased multi-function devices. General Services will have the vendor verify their data sanitization services in writing. The sanitization services must utilize the methods detailed in the Department of Defense (DoD) 5220.22-M, the National Industrial Security Program Operating Manual, or NIST SP 800-88, Guidelines for Media Sanitization. The services will provide proof of successful sanitization to DCF for audit purposes.

(8) Destruction Methods for Confidential and Federal Tax Information (FTI) Data. For digital FTI, the information owner and the information custodian will review, approve, track, document, and verify media sanitization of computer equipment containing Federal Tax Information (FTI) data per requirements in IRS Publication 1075, Tax Information Security Guidelines for Federal, State, and Local Agencies; Safeguards for Protecting Federal Tax Returns and Return Information. Media verification includes sampling sanitized media and confirming that a DCF employee witnessed that sanitization.

10. Media Use. The Department restricts portable information system media on DCF information systems or system components by policy and procedures. DCF program offices may create and own more restrictive or prohibitive policies and procedures for media use within their program office. Media Use also applies to mobile devices with information storage capability (e.g., smartphones, tablets) and restricts certain types of media on information systems, such as limiting/prohibiting the use of flash drives or external hard disk drives.

a. The Department prohibits portable storage devices in DCF business and information systems when such devices have no identifiable owner. For these devices, an identifiable owner (e.g., individuals, business units, or projects) is required to reduce the risk of using such technologies by specifying who is responsible and accountable for addressing known vulnerabilities in the DCF devices they are responsible for (e.g., malicious code).

b. The Department restricts the use of sanitization-resistant media in DCF business and information systems. Sanitization resistance applies to the capability to purge information from the media device. Certain media types do not support sanitization commands, or if supported, the devices do not have standardized support across the interfaces. Sanitization-resistant media include, for example, compact flash, embedded flash on boards and devices, solid-state drives, and USB removable media. Sanitization-resistant media held Restricted or Confidential data as per CFOP 50-27, Data Classification and Access Control, cannot be re-assigned but, if retired, must be destroyed per Department policy.

c. DCF program offices can employ technical and nontechnical safeguards (including policies, procedures, and rules of behavior) to restrict the use of information system media.

d. DCF program offices may restrict portable storage devices, for example, by using physical cages on workstations to prohibit access to specific external ports or disabling/removing the ability to insert, read or write to such devices.

e. DCF program offices may also limit the use of portable storage devices to only approved devices including, for example, devices provided by the Department, other approved business partners, and non-personally owned devices. Finally, DCF may restrict the use of portable storage devices based

on the type of device, for example, prohibiting the use of writeable, mobile storage devices and implementing this restriction by disabling or removing the capability to write to such devices.

f. Data loss prevention software is in place on the Department's network to encrypt DCF work files being moved or copied to removable media from DCF computers.

(1) Any DCF computer needing a DLP security policy exception for DCF business purposes must be vetted by an operationalized security review and documented in the DCF Statewide Help Desk Ticketing system. Then approved by the respective program office before being approved by the ISM, who is responsible for documenting the exception and the DCF business reasons the exception was approved.

(2) After approval has been received and documented, the computer receiving the exception will be identified ("tagged") within the Department's DLP software as a computer that has a DLP security policy exception.

(3) An automated monthly report of all DCF machines identified ("tagged") within the Department's DLP software as a computer that has a DLP security policy exception is generated on the first of each month and is emailed to the OITS Security Team's Distributed List and the Department's ISM for monthly review purposes.

g. DCF employee responsibilities include the following:

(1) Do not store sole record copies of Department information on workstations or mobile devices. The appropriate place for DCF records is a server with regular backups and a back-up library.

(2) Ensure applicable data retention requirements are met for information on Department-owned computer equipment.

(3) DCF employees shall take all reasonable precautions to protect mobile computing devices in their possession from loss, theft, tampering, unauthorized access, and damage:

(a) All Department laptops and mobile devices issued to end-users containing confidential information or data must employ encryption mechanisms to ensure unauthorized disclosure of confidential information or data is prohibited if the computer or mobile device is lost or stolen.

(b) If any confidential information or data resides on a computer or device, the computer or device must be encrypted and protected as if all the data were entirely identifiable information or data.

(c) DCF employees will not allow access to media in their custody by those not authorized as defined by their Department assigned roles.

(d) DCF employees will not allow mobile devices used outside of the Department's physical boundaries to be used by non-DCF resources (e.g., family members, friends).

(e) CFOP 50-2, Security of Data and Information Technology Resources, Chapter 4, Use of Wireless Technology and Mobile Devices, requires end-users to report lost or stolen mobile devices.

11. Media Downgrading. This control applies to all information system media subject to release outside of DCF, whether or not the media is considered removable. When applied to system media, the downgrading process removes information from the media, typically by security category or

classification level, such that the data cannot be retrieved or reconstructed. Downgrading of media can also involve ensuring that space on the media (e.g., slack space within files) is devoid of information.

a. DCF manages the downgrading of computer or information system equipment with no internal media or memory per CFOP 80-2, Property Management. The operating procedure that sets forth guidelines and policies for managing DCF-owned tangible property, including procedures for disposing of surplus property.

b. The Department must remove media from computers or information systems that require a downgrade. Media that has held only public data per CFOP 50-27, Data Classification and Access Control, can be sanitized per this operating procedure and reused internally by the Department. DCF owned media that held Restricted or Confidential must be destroyed and cannot be re-issued.

c. CFOP 50-27, Data Classification and Access Control, provides the security category and/or information classification levels of data contained on media. In preparation for the downgrading process and the access authorizations of the potential media recipients, that is to be re-assigned or destroyed, identifying who may handle the media for the sanitization or destruction processes.

d. The Department downgrades information system media containing Restricted or Confidential information before releasing to individuals without required access authorizations per applicable federal and state laws and DCF standards and policies. Downgrading of Restricted or Confidential information shall use approved sanitization tools, techniques, and procedures to transfer information confirmed to be unclassified from classified information systems to unclassified media.

12. Enforcement. Violations of information security policies and procedures may result in loss or limitations on the use of information resources, disciplinary action up to and including termination of employment or contractual relationship, and referral for civil or criminal prosecution as provided by law.

BY DIRECTION OF THE SECRETARY:

(Signed original *copy on file)*

COLE SOUSA
Chief Information Officer

SUMMARY OF REVISED, DELETED, OR ADDED MATERIAL

Annual review completed; no substantive changes.