1. **Purpose.** This operating procedure provides the minimum security requirements for media protection to prevent the loss of confidentiality, integrity, or availability of Department 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 selection of the cryptographic mechanisms used is based upon maintaining the confidentiality and integrity of the information.

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

   a. Any information not specifically identified as the property of other parties that is 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 and store confidential information or data on behalf of the Department are subject to review.

3. **References.**


   d. Chapter 74-2, Florida Administrative Code, “Florida Cybersecurity Standards.”

   e. IRS Publication 1075, “Safeguards Program.”

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


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

   i. NIST SP 800-53 r4, “Security Controls and Assessment Procedures for General Information Systems and Organizations.”
4. Definitions. For the purposes of this operating procedure, the following definitions shall apply:

a. Confidential Information and/or 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 device 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 the purposes of this operating procedure, the definition of employee includes any non-OPS temporary staff hired by the Department who have access to DCF IT resources.

f. Exempt Information. Information DCF is not required to disclose under Section 119.07(1), F.S., but which the Department is not necessarily prohibited 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 and in accordance with all the Department’s information handling procedures:

h. Information Owner. The manager of the business unit ultimately responsible for the collection, maintenance, and dissemination of a specific collection of information. Responsibilities include maintaining a reference list of their exempt and confidential and exempt information along with the associated applicable state and federal statutes and rules, and maintaining Department data in accordance with the 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 serve to provide appropriate access to and protect the confidentiality and integrity of information in compliance with Department and statewide policies and standards and in accordance with section 282.318, F.S., and Chapter 74-2, 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, but not limited to, USB drives, diskettes, magnetic tapes, external/removable hard disk drives, compact disks, and digital video disks.
I. Media Sanitization. One of the key elements in assuring confidentiality of information. A process to render access to target data on the media infeasible for a given level of effort. Clear, Purge, and Destroy are actions that can be taken to sanitize media:

1. **Clear.** Applies logical techniques to sanitize data in all user-addressable storage locations for protection against simple non-invasive data recovery techniques; typically applied through the standard Read and Write commands to the storage device, such as by 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 disintegration, incineration, pulverization, melting, and shredding. Disintegration, incineration, pulverization, and melting are designed to completely destroy the media.

m. **Mobile Device.** Any nonstationary electronic device with singular or multiple capabilities of recording, storing, and/or transmitting data, voice, video, or photo images. This includes but is not limited to laptops, personal digital assistants, pocket personal computers, MP3 players, smartphones, and video cameras.

5. **Enforcement.** Violations of information security policies and procedures may result in loss or limitations on 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.

6. **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 (electronic data/voice/video/image, microfilm, etc.), 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 business system and/or within a program office at DCF.

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

7. **Media Marking.** The Department restricts access to media based upon the classification system of the data the media contains per CFOP 50-27, Data Classification and Access Control. As part of data classification, business systems and/or program areas shall mark all information system media so that 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. All Department surplus PCs and any removed disk drives or other small removable storage devices must have a label applied that indicates the date the authorized personnel performed the data sanitization and the method used for data sanitization. If the media was sanitized by destruction, DCF
must maintain records of the destruction that include the date and the names of the authorized personnel who performed and witnessed the media destruction.

c. The Department must establish adequate controls to prevent disclosing FTI to other state agencies, tax or non-tax, or to 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).

8. Media Storage. The Department shall control and securely store all types of 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 accountability for all stored media.

b. Controlled areas are areas for which the Department provides sufficient physical and procedural safeguards to meet the requirements established 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 State of Florida to be in the public domain, to be publicly releasable, or to 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.

9. Media Transport. The Department protects and controls information system media during transport outside of controlled areas using applicable program office defined security safeguards, maintains accountability for information system media during transport outside of controlled areas, documents activities associated with the transport of information system media, and restricts the activities associated with the transport 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) that are transported outside of controlled areas 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 protections depending upon the mechanisms 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 have the technical ability to proactively encrypt external hard drives owned by their program office area. This ability is provided within the Microsoft workstation operating system; users can encrypt an external hard drive by right-clicking the drive within the Windows Explorer / Computer windows and selecting the Encrypt option.

f. Activities associated with transport include the actual transport as well as activities like releasing media for transport and ensuring that media enters the appropriate transport processes. For the actual transport, authorized transport and courier personnel may include individuals from outside the Department (e.g., U.S. Postal Service or a commercial transport 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 explicit 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 in accordance with 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 containing confidential information or data are transferred, 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 that is removed from the system. Such actions will be logged with details including the name of the user and the data that was copied. The Department shall implement tools to monitor and log or encrypt such actions.

10. Media Sanitization. To ensure compliance with rules pertaining to the disposition of confidential information, employees must ensure data sanitization prior to the disposal, surplus, reuse, or off site repair of any information technology resource.

a. Sanitization techniques and procedures in accordance with applicable federal and Department standards and policies are used. Sanitization mechanisms should always display strength and integrity respective to the security level and data classification level of the information.

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, Guidelines for Media Sanitization. These methods involve overwriting all data tracks at a minimum of three times, more 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 information cannot be retrieved or reconstructed.
(3) Sanitization techniques, including clearing, purging, bit level wiping, 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 destruction as a method is necessary when other methods cannot be applied to media requiring sanitization.

(5) DCF employees must request data sanitization support from the DCF Service Desk or their Regional Security Officer/Administrator. Prior to seeking data sanitization support, employees must backup and remove all documents and confidential information prior to releasing the information technology resource from their possession. Employees should contact the DCF IT Statewide Help Desk with any questions.

(6) Only authorized personnel shall prepare information technology devices that have contained confidential information for disposal, surplus, reuse, or off site repair. Authorized personnel shall document when, how, and what method was used for data sanitization. All surplus PCs and any removed disk drives or other small removable storage devices must have a label applied that indicates the date the authorized personnel performed the data sanitization and the method used for data sanitization.

(7) Multi-Function Devices. The Department shall ensure that the hard drives on all leased multi-function devices are sanitized at end of service. Whenever these devices are to go off-lease or be 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 on-site location until IT security staff take possession and sanitize or destroy the hard drives. When DCF does not option to own the hard drives on leased multi-function devices, General Services will have the vendor verify in writing that their data sanitization services utilize the methods detailed in Department of Defense (DoD) 5220.22-M, the National Industrial Security Program Operating Manual, or NIST SP 800-88, Guidelines for Media Sanitization, and that these 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 methods for computer equipment containing Federal Tax Information (FTI) data in accordance with requirements in IRS Publication 1075, Tax Information Security Guidelines For Federal, State and Local Agencies; Safeguards for Protecting Federal Tax Returns and Return Information. This includes sampling sanitized media to verify sanitization and that sanitization was witnessed by a DCF employee.

11. Media Use. The Department restricts the use of 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., smart phones, tablets) and restricts the use of certain types of media on information systems, for example, restricting/prohibiting the use of flash drives or external hard disk drives.

   a. The Department prohibits the use of 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 media. Certain types of media do not support sanitize commands, or if supported, the interfaces are not supported in a standardized way across these devices. Sanitization-resistant media include, for example, compact flash, embedded flash on boards and devices, solid state drives, and USB removable media. Sanitization-resistant media that has held Restricted or Confidential data as per CFOP 50-27, Data Classification and Access Control, cannot be re-assigned and if it is to be retired, it must be destroyed as 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 the use of portable storage devices, for example, by using physical cages on workstations to prohibit access to certain 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, devices provided by other approved business partners, and devices that are not personally owned. Finally, DCF may restrict the use of portable storage devices based on the type of device, for example, prohibiting the use of writeable, portable 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 first be vetted by an operationalized security review process 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 been granted 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 been granted 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 to 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 which has regular backups scheduled and a back-up library in place.

(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 end-user laptops and mobile devices containing confidential information or data that reside at an alternate work site must employ encryption mechanisms to ensure that confidential information or data may not be accessed 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 confidential 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) Report lost or stolen mobile devices as required by CFOP 50-2, Security of Data and Information Technology Resources, Chapter 4, Use of Wireless Technology and Mobile Devices.

12. Media Downgrading. This control applies to all information system media subject to release outside of DCF, whether or not the media is considered removable. The downgrading process, when applied to system media, removes information from the media, typically by security category or classification level, such that the information cannot be retrieved or reconstructed. Downgrading of media can also involve ensuring that empty space on the media (e.g., slack space within files being retained) is devoid of information.

a. At DCF, the downgrading of computer or information system equipment with no internal media or memory is managed by CFOP 80-2, Property Management, the operating procedure that sets forth guidelines and procedures for the management of DCF-owned tangible property, including procedures for the disposal of surplus property.

b. Media from computers or information systems to be downgraded must be removed. 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 classification level of the information to be removed from media preparing for the downgrading process and the access authorizations of the potential recipients of the media 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 prior to release to individuals without required access authorizations in accordance with applicable federal and state laws, and federal, state, 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.
BY DIRECTION OF THE SECRETARY:

(Signed original copy on file)

JOE VASTOLA
Chief Information Officer