STATE OF FLORIDA
DEPARTMENT OF
CHILDREN AND FAMILIES
TALLAHASSEE, September 23, 2025

CF OPERATING PROCEDURE
NO. 50-7

Systems Management

STATEWIDE OFFICE AUTOMATION STANDARDS

This document establishes the Department of Children and Families' (Department or DCF) policy and standards for office automation hardware and software per applicable laws, Executive Orders, regulations, standards, and guidelines. These standards are subject to change based on the State of Florida requirements and as the Department's needs change. This policy shall be reviewed and revised annually or when a significant change occurs, whichever occurs first; refer to Appendix A: Policy Review and Revision. The review will be performed by the department's Information Security Manager (ISM) or designee.

BY DIRECTION OF THE SECRETARY:

(*Signed copy on file*)

COLE SOUSA
Chief Information Officer

SUMMARY OF REVISED, DELETED, OR ADDED MATERIAL

Revised section 7 established the Department's Mobile Device Standards, renumbered sections 7 through 8 (8 through 9), revised exception request process throughout, updated workstation standards, including Appendix A: Policy Review and Revision chart to reflect the Department's current standardized and specialty software options.

This operating procedure supersedes CFOP 50-7, dated September 10, 2024.
OPR: ITS

Table of Contents

Page

1. Purpose. This document describes the Department's policy and standards for office automation hardware and software. These standards are subject to change based on the State of Florida requirements and as the Department's needs change.

2. Scope. All information technology resource users (DCF employees, contractors, vendors, and others) are responsible for adhering to this operating procedure. The Office Information Technology Services (OITS) is tasked with ensuring that only approved applications are used on computing devices within the organization.

3. Reference.

a. Section 282. 318, Florida Statutes (F. S.), "State Cybersecurity Act."

b. Chapter 60GG-2, Florida Administrative Code (F. A. C.), "Florida Cybersecurity Standards."

c. CFOP 60-45, Chapter 1, Recognition and Awards Program.

d. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 r 5, "Security and Privacy Controls for Information Systems and Organizations."

4. Definitions. For the purposes of this operating procedure, the following definitions shall apply:

a. Chief Information Officer. The duties of the Chief Information Officer (CIO) include the management and oversight of strategy and implementation for the usability of information technology and the business systems that support enterprise goals.

b. 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.

c. Information Security Manger/Officer (ISM). A person designated by the Secretary of the Department to report to the 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 60GG-2, F. A. C.

d. 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.

e. Mobile Computing Device. A computing device that has a small form factor such that it can easily be carried by a single individual; designed to operate without a physical connection (e.g., wirelessly transmit or receive information); includes a self-contained power source; and capable 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. Policy.

a. All office automation equipment or software purchased or installed must adhere to the standards published in this operating procedure unless an exception is granted; refer to paragraph 5(b)

for details. Purchase of office automation equipment or software must adhere to procurement policies; refer to CFOP 50-9, Procurement of IT Resources.

b. Non-standard products shall be considered on an exception basis only. The Program Office Director or delegate shall submit requests for an exception via the IT ticketing system (i.e., ServiceNow) to the Office of Information Technology Services (OITS) staff (i.e., Endpoint, Security and IT leadership) for review and approval before installation. The Department prohibits the procurement of mobile devices that Apple Business Manager (ABM) cannot enroll and manage. Wi-Fi-only models or devices purchased outside authorized channels (e.g., consumer retail) that prevent ABM enrollment are prohibited.

6. Workstation Standards.

a. New workstation (desktop or laptop) configurations must adhere to the DCF minimum standard configurations as follows:

(1) For most agency employees, a laptop with a 14” non-touch screen, an Ultra 5 processor, 32GB of RAM, a 256GB SSD drive.
(2) For investigative positions requiring signature capture technology, a 2-n-1 laptop with a 12-13” touch screen, an Ultra 5 processor, 32GB of RAM, and a 256GB SSD drive.
(3) For power users and OITS staff, a laptop with a 15” non-touch screen to include a 10 key in addition to standard keyboard, an Ultra 5 processor, 32GB of RAM, and a 512GB SSD drive.
(4) For kiosk usage, an Intel NUC with an Ultra 5 processor, 32GB RAM, and a 256GB SSD drive.
(5) For limited workspace/cubicle size areas, a desktop of the micro form factor, with an Ultra 5 processor, 32GB of RAM, and a 256GB digital drive.

b. All workstations shall be members of Active Directory unless used as a public kiosk computer, for testing vacancy candidates or for training demonstrations.

c. All workstations (desktops, laptops, or notebooks) purchased must be capable of running the standard software applications listed in paragraph 8. The minimum configuration for a particular workstation must be based on what the employee needs to perform their job duties, taking into consideration not only standard software but any other applications or special software that the employee is required to use. Headquarters, institution, or region IT staff are responsible for determining the necessary configuration.

At purchase, workstations must have a minimum 3-year warranty provided by the manufacturer. No additional maintenance contracts shall extend the warranty secured that was of original purchase. In addition, all workstations must include “hard drive retention” to ensure that the manufacturer does not receive failed drives containing sensitive data.

d. Employees are permitted to have only one assigned laptop or desktop computer and one assigned mobile phone. The Program Office Director or delegate shall submit requests for exceptions to OITS staff; refer to paragraph 5(b) for details, including the employee’s acknowledgment of the following:

(1) The computing device must be kept in working condition with all associated peripherals and chargers.
(2) The computing device must only be used for conducting DCF business.
(3) If the computing device is a laptop or desktop computer, it must be placed online and connected to DCF’s network at the office or my residence via VPN no less than once every ten (10) days and kept online for no less than one (1) hour. This is necessary for the computer to maintain its trust relationship with Active Directory and to receive updates. If the device is an iPad, it must be turned

on no less than once every ten (10) days and kept online for no less than one (1) hour. This is necessary for the iPad to maintain its trust relationship with Active Directory and to receive updates.

(4) The computing device must be made available, upon request, for annual inventory or maintenance.

(5) Failure to adhere to the above may result in an inability to use the computing device on DCF's network. Should this occur, employee must submit a ticket to the Help Desk and understand that the resolution is not a priority because the employee's primary computing device is unavailable.

(6) Failure to adhere to the above may also result in the loss of this privilege of having an additional computing device.

7. Mobile Device Standards. All mobile devices purchased by the Department shall:

a. Be devices manufactured by Apple (i.e., iPads, iPhones).

(1) Include Verizon LTE service (Wi-Fi-only models are not permitted). To identify and eliminate connectivity issues to Department networks or systems, Wi-Fi-only iPad devices shall be coordinated with OITS before purchase; refer to paragraph 5(b) for details.

(2) Be eligible for and enrolled in Apple Business Manager (ABM) at the time of purchase.

(3) Be supervised and managed through the Department's mobile device management (MDM) platform before deployment.

b. Be a neutral color (e.g., black, grey, silver).

c. Protected by a ruggedized, neutral-colored case (i.e., Otterbox, UAG).

d. Device upgrades must remain on the same assigned line; no reassignment of upgraded devices to a different line is allowed ('buddy upgrades').

e. Exceptions to these requirements must be approved by OITS staff; refer to paragraph 5(b) for details, which includes compliance with CFOP 50-9.

8. Software Standards.

a. Standard Software. The software listed below has been adopted as standard software and therefore does not require justification for use, purchase, or upgrade.

Word processing	Microsoft Word
Spreadsheet	Microsoft Excel
Graphics	Microsoft PowerPoint
Integrated office suite	Microsoft Office
Browser	Microsoft Edge
Anti-Virus	Microsoft Defender
Endpoint Management	Tanium
Messaging/calendaring	Outlook Office 365
Encryption	Microsoft BitLocker
Collaboration	Microsoft Teams

b. Other Standard Software. The software listed below has been adopted as standard software and therefore does not require justification to use. It is available at no cost without a procurement request.

Portable document format (. pdf) reader	Adobe Acrobat Reader

c. Specialty Software. The software listed below has been adopted as standard specialty software and therefore requires justification of the need to use. The justification must be submitted as part of the procurement process.

Flowcharting	• Visio Standard (general use) via Program Office Managed Subscription • Visio Professional (detailed or technical use) via Program Office Managed Subscription
Reporting	Power BI
Portable document format (. pdf)	Adobe Acrobat via Program Office Managed Subscription
Sanitizing storage devices	Blancco Data Erasure

d. Non-standard software. Any exceptions to use other software not listed in paragraphs a-c must be requested by the Program Office Director or delegate; refer to paragraph 5(b) for details.

9. Peripherals. Contact your local OITS manager to discuss needs for any hardware or software not listed below.

a. Monitors for employee usage should be 24” – 32” in size with DisplayPort and HDMI connections as well as being height adjustable. Requests for larger monitors requires approval from the Program Office Director or their delegate. Smaller monitors can be purchased if required for fitment in kiosk-type furniture cabinets.

b. Bluetooth Earbuds may not exceed $100 in cost as outlined in CFOP 60-45 Chapter 1.

c. Copier/Multi-Function Devices are limited to two vendors for Region/Facility/HQ due to support complexities.

Appendix A: Policy Review and Revision

DATE	VERSION	ACTION TYPE	DESCRIPTION
07/21/2021	1.0	Annual Review and Revision (ARR)	Revised ‘Reference’ section and renumbered sections 3 through 8.
10/26/2022	2.0	ARR	Revised paragraphs 6 through 8 to reflect current office automation standards.
11/01/2023	3.0	ARR	No substantive changes.
09/10/2024	4.0	ARR	Updated Software Standards, section 7 subsections a and c.
08/20/2025	5.0	ARR	Established policy and standards for mobile devices used by Department staff, renumbered paragraphs 7 through 8 respectively to 8 and 9, revised exception request process throughout, and added Appendix A: Policy Review and Revision chart.