Systems Management

STATEWIDE OFFICE AUTOMATION STANDARDS

This operating procedure establishes the Department of Children and Families' (Department or DCF) 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.

BY DIRECTION OF THE SECRETARY:

(*Signed copy on file*)

COLE SOUSA
Chief Information Officer

SUMMARY OF REVISED, DELETED, OR ADDED MATERIAL
November 1, 2023: Annual review and revision completed, no substantive changes.

Table of Contents

1. <u>Purpose</u>. This operating procedure establishes the Department of Children and Families' (Department or DCF) 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. <u>Scope</u>. 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. <u>Reference</u>.

> 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. <u>Definitions</u>. For the purposes of this operating procedure, the following definitions shall apply

> a. <u>Chief Information Officer</u>. 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. <u>Employee</u>. 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. <u>Information Security Manger/Officer (ISM)</u>. 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. <u>Information Technology Resources</u>. 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. <u>Mobile Computing Device</u>. 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. <u>Policy</u>.

> 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 in writing by the

Program Office Director or delegate and forwarded to the DCF CIO. Purchase of office automation equipment or software must adhere to procurement policies.

b. Non-standard products will be considered on an exception basis only. Any requests for an exception to Department standards must be made in writing, approved by the Program Office Director or delegate, and forwarded to the DCF CIO for review.

6. <u>Workstation Standards</u>.

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

(1)   For most agency employees, a laptop with a 14" non-touch screen, an Intel i5 processor, 16GB 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 Intel i5 processor, 16GB 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 Intel i7 processor, 32GB of RAM, and a 512GB SSD drive.

(4)   For kiosk usage, an Intel NUC with an Intel i5 processor, 8GB RAM, and a 256GB SSD drive.

(5)   For limited workspace/cubicle size areas, a desktop of the micro form factor, with an Intel i5 processor, 16GB 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 7 below. 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 may only have one assigned laptop or desktop computer and one assigned mobile phone. Requests for exceptions must be made in writing, approved by the Program Office Director or delegate, and forwarded to the DCF CIO, 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 10 days and kept online for no less than 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 10 days and kept online for no less than 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 resolution is not a priority because employee's my primary computing device available for use.

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

7. <u>Software Standards</u>.

a. <u>Standard Software</u>. 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	McAfee VirusScan
Messaging/calendaring	Outlook Office 365
Encryption	Microsoft BitLocker
Collaboration	Microsoft Teams

b. <u>Other Standard Software</u>. 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. <u>Specialty Software</u>. 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
	Qlik

| Portable document format (.pdf) | Adobe Acrobat via Program Office Managed Subscription |
| Sanitizing storage devices | Blancco Data Erasure |

      d. <u>Non-standard software</u>. Any exceptions to use other software not listed in paragraphs a-c must be made in writing, approved by the Program Office Director or delegate, and forwarded to the DCF CIO for review to use non-standard software.

8. <u>Peripherals</u>. 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.