

CF OPERATING PROCEDURE
NO. 50-30

STATE OF FLORIDA
DEPARTMENT OF
CHILDREN AND FAMILIES
TALLAHASSEE, December 22, 2025

Systems Management

IDENTITY AND ACCESS MANAGEMENT (IAM)

This document establishes the Department of Children and Families (Department) access control policy and processes described herein by which information technology (IT) resources is limited to authorized users, processes, or devices and to authorized activities and transactions.

BY DIRECTION OF THE SECRETARY:

(Signed copy on file)

COLE SOUSA
Chief Information Officer

SUMMARY OR REVISED, DELETED, OR ADDED MATERIAL

The annual review and revision were completed, and the operating procedure was revised throughout to reflect the Department's current access control policy and processes.

TABLE OF CONTENTS

	Page
1. Purpose	3
2. Scope	3
3. Authority.....	3
4. Policy Statement.....	3
5. Organizational Security.....	3
6. Definitions.....	4
7. Identity and Access Management Compliance Principles	6
7.1. Manage Identities and Credentials.....	6
7.2. Periodic Monitoring of Identities and Credentials.	8
7.3. Manage Physical Access	8
7.4. Manage Remote Access	9
7.5. Cybersecurity Standards and Best Practices	9
7.6. Identity Management	9
7.7. Risk Management.....	9
8. Identity and Access Management Governance	9
8.1. Roles and Responsibilities	10
8.2. Audit and Monitoring:	11
8.3. Change Management and Release Management:	11
8.4. Incident Response and Remediation:.....	11
8.5. Reporting	11
8.6. Policy Acknowledgement	11
Appendix A: Policy Review and Revision	12

1. Purpose. This document establishes the Department of Children and Families (Department or DCF) policy and describes a uniform process for Identity and Access Management (IAM) for Department system users and IT resources, per applicable forms, including but not limited to a digital Access Authorization Request (AAR)-138 form or a manual Department of Children and Families (CF)-138 form. These official documents outline the creation, modification, and deactivation of Department IT resources in accordance with applicable laws, Executive Orders, regulations, directives, policies, standards, and guidelines.

2. Scope. This operating procedure applies to all system users accessing Department information technology (IT) resources or data including but not limited to all information technology resources used to support or implement the mission of this Department and any other automated data processing systems in our custody whether owned, purchased, contracted from or to, or leased by the Department.

3. Authority.

- a. Rule Chapter 60GG-2, Florida Administrative Code (FAC), *Florida Cybersecurity Standards*.
- b. Department of Children and Families Operation Procedure 50-2, *Security of Data and Information Technology Resources*.
- c. Section 282.318, Florida Statutes, *State Cybersecurity Act*.
- d. 45 CFR Parts 160 and 164, Subparts A and C, Health Information Portability and Accountability Act (HIPAA) Privacy and Security Rules.
- e. The Centers for Medicare & Medicaid Services (CMS) Acceptable Risk Controls for Affordable Care Act (ACA), Medicaid, and Partner Entities: Volume 1, 1.02 Requirements, (04-2025).
- f. 5 U.S.C. 552a, *Privacy Act of 1974 - Electronic Information Exchange Security Requirements and Procedures for State and Local Agencies Exchanging Electronic Information with the Social Security Administration (SSA)*.
- g. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 r5, *"Security and Privacy Controls for Information Systems and Organizations."*
- h. Internal Revenue Services (IRS), Publication 1075, Tax Information Security Guidelines for Federal, State and Local Agencies, (11-2021).

4. Policy Statement. The Department shall hold system users accountable for adhering to policies and procedures that protect confidential data/information from unauthorized modification, destruction, use, or disclosure, including but not limited to Federal Tax Information (FTI), Social Security Numbers (SSNs), and Personal Health Information (PHI). Access to Department resources is granted on the principle of least privilege and enforcing the separation of duties best practice that no individual controls the entire process. The Information Security Manager or their delegate shall review and revise the IAM policy and procedures described herein annually (every 365 days) or when a significant process change occurs, whichever occurs first; refer to Appendix A: Policy Review and Revision.

5. Organizational Security.

- a. Chief Information Officer (CIO). Oversight, guidance, final review, and approval.

b. Deputy CIO. Oversight of Enterprise Infrastructure Resources.

c. Information Security Manager (ISM). Oversight, review, and compliance.

d. Information Security Operations & Administration Team. Oversight of all OITS Identity and Access Management Procedures for Employees, Contractors, and Community Care Based (CBC) organizations.

e. Hiring Manager (or designee). Responsible for approving employee and contractor requests for accessing any information system.

f. Human Resources Liaison. Facilitates and assists with Human Resource related activities (e.g., new hires, reassignment, and separation) and provides staff rosters for the physical access review process.

g. Program Area. Responsible for ensuring all employees and contractors adhere to this operating procedure.

6. Definitions. Terms used in this operating procedure are defined below.

a. Access Management. The IT Security Management process is responsible for allowing users access to and use of IT services, data, or other assets. Access management helps protect the confidentiality, integrity, and availability of assets by ensuring that only authorized users can access or modify them. Access management implements information security management policies (also referred to as rights management or identity management).

b. Account Provisioning. The process of granting permissions by creating or changing user accounts or privileges as necessary includes disabling and deleting accounts.

c. Cybersecurity. The protection afforded to an automated Information System to attain the applicable objectives of preserving the confidentiality, integrity, and availability of Data, information, and information Technology resources.

d. Elevated (Privileged) Access. The cybersecurity principle that requires, when an individual who does not normally have access to a secure system requires access, they will either be given temporary access with a clear start and end date, or they will gain access through an intermediary who has access to the system or data.

(1) Privileged Account(s). Accounts created for system users who are authorized (trusted) to perform administrative tasks to manage and support critical systems and application functions that general (standard) users are not permitted to perform (e.g., special access to software application or source code), requires additional training, and must acknowledge the Department's Acceptable Use Policy (AUP).

(2) Administrative accounts include but are not limited to the following roles, per federal guidance:

- a) Database Administrators
- b) Application Technical Support
- c) Operational Support
- d) Application Administrators
- e) System Developers and Maintainers
- f) System/Network Administrators

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 Department IT resources, including contracted staff and contracted vendor staff.

f. Hiring Manager. The director, manager and/ or supervisor engaged in hiring a new employee.

g. Identity and Access Governance (IAG) Tools. Applicable tools used to automate the provisioning into authentication repositories, including but not limited to:

(1) Okta. A multifactor authentication (MFA) app that permits secure log-in to available applications for Department employees and contractors. A Single Sign On (SSO), authentication scheme that allows a user to log in with a single set of credentials to access multiple applications and websites.

(2) Azure Active Directory (AD). A cloud-based identity and access management service developed by Microsoft. AD creates a unique identifier for each individual employee or contractor through their Microsoft account. The Department compiles AD with OKTA and SailPoint to facilitate the IAM process.

h. Information Security Manager. The Information Security Manager (ISM) is the person designated by the Secretary of the Department to administer the Department's information technology security program and serve 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 §282.318, Florida Statutes, and Chapter 60GG-2, F.A.C.

i. Information System. Any information resources organized for the collection, processing, creation, maintenance, use, sharing, dissemination, or disposition of digital information.

j. Information Technology Resources (Technology Assets). Equipment, hardware, software, firmware, programs, systems, networks, infrastructure, media, and related material used to automatically, electronically, and wirelessly collect, receive, access transmit, display, store, record, retrieve, analyze, evaluate, process, classify, manipulate, manage, assimilate, control, communicate, exchange, convert, converge, interface, switch, disseminate information of any kind or form.

k. Office of Information Technology Services (OITS). Department of Children and Families Office of Information Technology Services.

l. Principle of Least Privilege (PoLP). The requirement that each business system process, a user, or program must be able to access only the information and resources that are necessary for its business legitimate purpose.

m. Separation of Duties. The principle that no user should be given enough privileges to misuse the system on their own, and process that involves dividing critical tasks and responsibilities among different individuals to create a system of checks and balances. No single individual should have complete control or authority over a process from start to finish.

n. System Owner(s). The entity that owns the data and that has the primary responsibility for decisions relating to a particular data processing system's specifications and usage.

7. Identity and Access Management Compliance Principles. The Department is committed to establishing a comprehensive operational framework, including standards and deliverables, which maximize the confidentiality, integrity, and availability of information technology (IT) resources. The Department shall manage identities and credentials for authorized devices and users to ensure all Department-owned systems shall adherence to industry standards and best practices.

7.1. Manage Identities and Credentials. Control measures shall, at a minimum include authentication token(s) unique to the individual. The Department shall:

- a. Require that all Department-owned or approved computing devices, including Mobile devices, use unique User Authentication.
- b. Require user to log off or lock their workstations prior to leaving the work area.
- c. Require inactivity timeouts that log-off or lock workstations or sessions.
- d. Locked workstations or sessions shall require User Authentication with an authentication token(s) unique to the individual to reestablish access.
- e. When applicable sole password authentication token(s) use complex passwords.
- f. Administer access to systems and data based on documented authorizations and facilitate periodic review of access rights with information owner(s) and/or Program Office area(s). Frequency of reviews shall be based on system categorization or assessed risk per section 7.2, Periodic Monitoring of Identities and Credentials.
- g. Establish access disablement and notification timeframe for system users separations via an approved ticketing system, per [CFOP 50-2, Chapter 2](#).
- h. Ensure IT access is removed when the IT Resources are no longer required, per item g.
- i. Require multi-factor authentication (MFA) for access to Department IT resources, including but not limited to systems with a categorization of moderate or high, which may contain exempt or confidential information. When IT technologies permit, include MFA at the application-level or single sign-on (SSO).

7.1.1. Permanent and Specialty Accounts (i.e., Temporary and Emergency). The Department shall define, establish, and support the management of system accounts based on, but not limited to, access privileges, duration, and other attributes (i.e., restriction on time of day, day of week, and point of origin).

a. Permanent Accounts. The Department shall issue permanent accounts with no specified end date to system users who require ongoing access to IT resources.

b. Specialty Accounts. The Department shall issue specialty accounts when system access is required for a specified timeframe (i.e., Florida Auditor General audits) or crisis situations (i.e., declared disasters, unplanned event) may bypass the account activation process described herein and in CFOP 50-2.

(1) Temporary Accounts. The Department shall establish temporary accounts for system users who do not require ongoing system access to perform their job duties. Designed point of contacts shall submit AAR documents via the centralized ticketing system repository. The IAM team (designee)

shall provision the account with six (6) months or less of system access. Temporary accounts (network/application-levels) shall automatically disable upon the specified end date.

(2) Emergency Accounts. The Department shall establish emergency accounts in response to crisis situations when a rapid account activation is necessary. Emergency accounts creation and deactivation shall be documented in a centralized ticketing system repository. The accounts shall remain active until the Department declares that the crisis has concluded; then, within 96 hours from that date, the Department shall terminate access to the emergency account.

7.1.2. Provisioning/Deprovisioning Responsibilities. A member of the IAM Team shall be assigned to review each IT Service Request created by the AAR-138 submission or a CF-138 for thoroughness and accuracy. Incomplete forms shall be returned/rejected, for example, additional comment field should not contain, 'Please mirror employee 'John Doe's' account, and complete forms shall be processed accordingly.

a. Account Creation and Modification. Access to the appropriate Department IT resources shall be established including but not limited to Department email, file folders, printers, and applications (i.e., internal and external).

(1) New Hire. Select this option to add the individual to Department IT resources stated in section 7.1.1(a). Do not select 'New Hire' option, if the individual has an existing DCF email address or Active Directory (AD) account.

(2) Existing. Select this option when an individual has existing IT resource accounts, that require but not limited to the following:

a) CHANGE. The individual needs updates to demographic (i.e., name, ssn, dob), access or security level.

b) SUSPEND. Account(s) require temporary hold.

c) TRANSFER. The individual's administrative structure changes (e.g., Program Office, work location, supervisor).

b. Separation. To terminate ALL access to Department IT resources, select 'Separation,' complete the appropriate fields, and **list all** system/data accounts that require deactivation, including any Administrative Accounts and external accounts (i.e., DAVID, CCIS, CONNECT, SUNTAX, FLMMIS), refer to CFOP 50-2, Chapter 2 for deboarding (separation) notification requirements.

NOTE: For essential Department systems (i.e., FSFN) that require continuous monitoring, the credentials of separating employees shall be suspended (locked) until management can reassign their caseload. The suspension of the credentials prohibits further system access. The Department has established a process to monitor and reassign unmanaged FSFN caseloads, updating credentials from suspension to deactivated status.

7.1.3. Network Accounts and Access Protocols. All Department system users shall adhere to authentication protocols and use complex passwords when supported by technology capabilities.

a. Email Address Criteria.

(1) A maximum of 64 characters before @myflfamilies.com includes, but not limited to, letters, periods, spaces, numbers, and hyphens.

(2) The standard email format is the employee's given (i.e., legal) name (i.e., birth certificate, social security card, VISA) FirstName.LastName@myflfamilies.com. When more than one (1) employee has the same first and last name, the IAM group will create a unique DCF email address for each subsequent individual.

(3) Department email addresses shall not use nicknames unless established before this policy (grandfathered in). If an employee leaves the Department and returns, the exception above no longer applies.

NOTE: For all Department-provisioned accounts (e.g., email, Active Directory (AD), application-level), including external accounts (i.e., DAVID, FLMMIS, CONNECT), the demographic information shall be consistent across all accounts.

b. Password Configuration Criteria. AD (network level) account shall have a minimum of 14 characters that include three (3) of the four (4) characteristics listed below:

- (1) At least one uppercase letter
- (2) At least one lowercase letter
- (3) One numeric character, and
- (4) A special symbol (i.e., @, #, \$, %, &)

c. Password Reset/History Configuration. AD passwords shall adhere to the following age/history standards:

- (1) Maximum age – 90 days
- (2) Minimum age – one (1) day
- (3) Cannot reuse the last ten (10) passwords

7.2. Periodic Monitoring of Identities and Credentials. The Department shall conduct periodic review of system accounts (general and privileged) per state and federal compliance standards. General user accounts have authorization to access, view, or edit the information within the application screen. Privileged user accounts have authorization to access, view, or edit the source code within the application platform.

a. Periodic Account Reviews. The Department shall conduct an annual review of general and privileged user accounts authorized to access, view, or edit application platforms that contain confidential or exempt information, including but not limited to Federal Tax Information (FTI), Personal Identifiable Information (PII), and Personal Health Information (PHI). The Department shall review general accounts at a minimum of every 365 days (once a year), and privileged accounts shall be reviewed at a minimum of every six (6) months (twice a year).

b. Internal Department Employee Accounts. The Office of Information Technology Services (OITS) will assist information owner(s) and/or Program Office area(s) to facilitate the review of Department employee accounts by importing account information into an IAM tool and providing status reports.

c. External (non-Department) User Accounts. OITS staff shall assist information owner(s) and/or Program Office area(s) to facilitate a review of Department IT resource accounts granted to non-Department (i.e., Department of Revenue, Department of Juvenile Justice, etc.) account holders by:

- (1) Providing a roster of external user accounts.
- (2) The roster shall contain data elements deemed necessary to conduct a thorough review of access privileges.
- (3) The information owner(s) and/or Program Area(s) are responsible for facilitating the validation of access privileges and retaining evidentiary information.

7.3. Manage Physical Access. The Department shall manage and protect physical access to assets by establishing controls that shall:

a. Protect IT Resources from environmental hazards (e.g., temperatures, humidity, dust, and faulty power) per manufacturer specifications.

- b. Restrict physical access to IT facilities and equipment under the Department's p.
- c. Define physical controls that are appropriate for the size and criticality of the IT Resources.
- d. Describe physical access to information resource facilities and equipment that is limited to authorized personnel only.
- e. Define visitor access protocols, including documentation procedures, and require visitors to be accompanied by authorized personnel in locations housing systems categorized as moderate or high impact.
- f. Incorporate network segregation to protect the integrity of the network.

7.4. Manage Remote Access. The Department shall:

- a. Establish protocols to securely manage, monitor, and document remote access.
- b. Define method by which system users may use to remotely connect computing devices to the Department's internal network.
- c. Including but not limited to system containing exempt, or confidential and exempt data, establish data sharing agreement (DSA) template, centralized document routing and tracking system, including an online repository for all Department agreements.

The DSA template consists of but not limited to standard reporting protocols for unauthorized disclosure and misuse notification processes.

7.5. Cybersecurity Standards and Best Practices. The Department shall ensure that access permissions and authorizations, are managed, by incorporating the principle of least privileged and separation of duties. In doing so, the Department shall:

- a. Execute interconnection security agreements to authorize, document, and support continual management of inter-agency connected systems; refer to CFOP 50-26, DSA.
- b. Manage access permissions by incorporating the 'principles of least privilege and separation of duties.'
- c. Provision all system user access to Department IT Resources based on the security controls in Section 7.4.b.
- d. Restrict and monitor the issuance of elevated privileges with the ability to bypass system and application controls.

7.6. Identity Management. The Department shall proof and bond identities to credentials and assert in interactions when appropriate. The Department shall accept Personal Identity Verification (PIV) credentials from other federal agencies applies to both logical and physical access control systems.

PIV credentials are those issued by federal agencies (i.e., Internal Revenue Services, Social Security Administration) that conform to FIPS Publication 201 and supporting guidelines.

7.7. Risk Management. The Department shall authenticate users, devices, and other assets commensurate with the risk of the transaction. The Department utilizes cryptographic mechanisms to protect IT resources from unauthorized commands and the replay of authorized commands.

8. Identity and Access Management Governance

a. Governance Framework: The Department establishes a Governance Framework to ensure effective management and oversight of the IAM Guiding Principles. The Governance Framework outlines the roles, responsibilities, policies, and processes related to within the Department.

b. Steering Committee: The Steering Committee is responsible for providing strategic guidance and oversight of initiatives and composed of key stakeholders, including but not limited to representatives from the Office of Information Technology Services (OITS), Program Areas, Human Resources, and Legal. The committee meets regularly to review mission critical initiatives (e.g., policies, cybersecurity risks, and make decisions regarding implementations and enhancements) and facilitates several functions.

(1) Executive Governance Board reviews all procurement requests; refer to CFOP 50-9 for details.

(2) Information Technology Board, which includes the CIO, will review, and approve allocation of resources, operating procedures, and automation standards for information technology related initiatives; refer to CFOP 50-9 for details.

(3) Cybersecurity Steering Committee assesses cybersecurity rating scores of third-party stakeholders; refer to CFOP 50-9 for details.

8.1. Roles and Responsibilities: The Governance Framework defines the roles and responsibilities of individuals involved in processes. These roles include but are not limited to:

a. Chief Information Officer (CIO): The CIO provides oversight and guidance for initiatives and ensures their alignment with the Department's overall IT strategy and goals.

b. Deputy CIO: The Deputy CIO assists the CIO in providing oversight on security policies and initiatives.

c. Information Security Manager (ISM): ISM serves as the process owner for activities and is responsible for developing and implementing policies, procedures, and controls. The ISM works closely with other stakeholders to ensure compliance and effectiveness.

d. Identity and Access Management Administrator: The Administrator is responsible for the day-to-day administration of systems and processes, including but is not limited to user provisioning, access requests, access reviews, and user lifecycle management.

e. System Owners: System Owners have the primary responsibility for making decisions regarding access to their respective systems. They work with the Administrator to define access requirements and ensure that access is granted based on the principle of the least privilege.

f. Program Area Representatives: Program area representatives are responsible for ensuring that employees and contractors within their respective areas comply with policies and procedures. They collaborate with the Administrator to address access-related issues and provide necessary approvals for access requests.

g. System Administration and Security Administration: The roles of system administrators and security administrators are distinct and segregated to enforce separation of duties. System administrators have administrative privileges to manage and maintain system functionality, while security administrators oversee access controls, user roles, and security policies. This separation prevents conflicts of interest and unauthorized modifications to access permissions.

8.2. Audit and Monitoring: The responsibility for auditing and monitoring IAM processes is separate from the operational roles involved in access provisioning and management. Independent auditors or a dedicated internal audit team perform periodic reviews of access controls, user activity logs, and system configurations to detect anomalies, identify compliance gaps, and ensure adherence to IAM policies. This separation adds an additional layer of oversight and reduces the risk of fraudulent activities going unnoticed.

8.3. Change Management and Release Management: The organization follows separate change management and release management processes, each with its own set of responsibilities and controls. Change management focuses on assessing, approving, and implementing changes to the IAM system, while release management deals with the deployment and rollout of system updates and enhancements. This separation minimizes the risk of unauthorized or untested changes impacting system integrity.

8.4. Incident Response and Remediation: The incident response process includes separate roles for incident detection, analysis, containment, and remediation. These roles are carried out by different individuals or teams to prevent a single person from having complete control over incident handling. For example, security analysts may be responsible for incident detection and analysis, while IT administrators handle system remediation. This segregation ensures a comprehensive and impartial response to security incidents.

8.5. Reporting: Establish clear reporting channels for users to report any issues, such as suspicious access requests, unauthorized access, or potential policy violations. These channels can include dedicated email addresses, helpdesk support, or incident reporting systems. Users are encouraged to report any security concerns promptly to facilitate timely investigation and remediation.

8.6. Policy Acknowledgement: Users are required to acknowledge and sign off on identity and access management policies and procedures to signify their understanding and compliance. This ensures that users are aware of their responsibilities and the consequences of non-compliance.

Appendix A: Policy Review and Revision

Date	Version	Action Type	Description
06/15/23	1.0	New operation policy	Established the IAM policy and processes.
08/01/24	2.0	Annual Review/Revision (ARR)	Added the State of Florida Cybersecurity Standards (SFCS).
11/17/25	3.0	ARR	Revised IAM policy/processes throughout to comply with CMS ARC-AMPE security control standards.