STATE OF FLORIDA
DEPARTMENT OF
CHILDREN AND FAMILIES
TALLAHASSEE, August 1, 2024

CF OPERATING PROCEDURE
NO. 50-30

Systems Management
IDENTITY AND ACCESS MANAGEMENT (IAM)

This operating procedure established the Department of Children and Families (Department) access control processes 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

August 1, 2024: The annual review and revision were completed, and the operating procedure was revised throughout to align with Protect (PR), Identity Management, Authentication, and Access Control (AC) State of Florida Cybersecurity Standards (SFCS). This operating procedure supersedes CFOP dated, June 21, 2023.

TABLE OF CONTENTS

1. Purpose. This operating procedure establishes a uniform process for Identity and Access Management (IAM) for Department system users, per applicable federal laws, state statutes, and administrative code.

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) Minimum Acceptable Risk Standards for Exchanges (MARS-E) 2.2 Requirements.

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. This policy establishes the cybersecurity standards per applicable federal and State laws, Executive Orders, directives, regulations, policies, standards, and guidelines. The Department shall hold system users accountable for adhering to policies and procedures which protect confidential data/information from unauthorized modification, destruction, use, or disclosure, including but not limited to Federal Tax Information (FTI). Access to Department resources is granted on the principle of least privilege and enforces the separation of duties so that no individual controls the entire process. Every 365 days or when a significant process change occurs, whichever occurs first, this policy and the resultant procedures should be reviewed and revised.

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.

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 the 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 Rule 60GG-2.003(1).

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 Use to disengage.

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). Frequency of reviews shall be based on system categorization or assessed risk.

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 is no longer required, per item g.

i. Require multi-factor authentication (MFA) for access to Department networks that have a categorization of moderate, high, or contain exempt, or confidential and exempt information. When IT technologies permit include MFA at the application-level.

j. Require MFA for access to Privileged Accounts.

7.2. 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.

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.

7.3. 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.

7.4. 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.

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.

7.5. Protect System Integrity. The Department shall ensure that network integrity is protected, incorporating network segregation and segmentation where applicable.

7.6. Identity Management. The Department shall proof and bond identities to credentials and assert in interactions when appropriate.

7.7. Risk Management. The Department shall authenticate users, devices, and other assets commensurate with the risk of the transaction.

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.