STATE OF FLORIDA
DEPARTMENT OF
CHILDREN AND FAMILIES
TALLAHASSEE, August 09 2023

CF OPERATING PROCEDURE
NO. 50-31

System Management

POLICY on PRIVILEGED ACCESS to INFORMATION TECHNOLOGY RESOURCES

This operating procedure establishes the Department's policy for obtaining privileged access to information technology resources and outlines the review and approval of privileged authorization to IT Resources.

BY DIRECTION OF THE SECRETARY:

(Signed copy on file)

COLE SOUSA
Chief Information Officer

SUMMARY OF REVISED, DELETED, OR ADDED MATERIAL
August 7, 2023: New operating procedure.

TABLE OF CONTENTS

1. Purpose. The purpose of this operating procedure is to establish the policy and describe the Department of Children and Families (Department) procedures for receiving privileged access to departmental resources under the authority of the Office of Information Technology Services (OITS) Chief Information Officer (CIO) authority.

2. Scope. This operating procedure applies to all Department staff with privileged access to IT resources.

3. Authority.

a. Section 282.318, Florida Statutes (FS), *State Cybersecurity Act*.

b. Section 501.171, FS, *Security of Confidential Personal Information*.

c. Rule Chapter 60GG-2, Florida Administrative Code (FAC), *Florida Cybersecurity Standards*.

d. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 r5, *Security and Privacy Controls for Information Systems and Organizations*.

e. 45 CFR Parts 160 and 164, Subparts A and C, *Health Information Portability and Accountability Act (HIPAA) Privacy and Security Rules*.

f. The Centers for Medicare & Medicaid Services (CMS) *Minimum Acceptable Risk Standards for Exchanges (MARS-E) 2.2 Requirements*.

g. 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).

h. Internal Revenue Service (IRS), Publication 1075, *Tax Information Security Guidelines for Federal, State and Local Agencies, Rev. 11-2021*.

i. CFOP 50-2, *Security of Data and Information Technology Resources*.

j. Department Standard Operating Procedure (SOP) S-4, *Computer Security Incident Response Team (CSIRT) Operating Procedures*

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

a. Employee (Staff). 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 this operating procedure, the definition of employee includes any non-OPS temporary staff hired by the Department. They have access to Department information technology resources, including contracted staff and contracted vendor staff.

b. Principle of Least Privilege (POLP). The cybersecurity practice under which users or processes have the most restrictive privileges necessary to perform routine job responsibilities.

c. Privileged (Elevated) Access. Access allows an individual to take actions affecting computing systems, network communication, or the accounts, fields, data, or processes. Typically, system administrators, network administrators, or other employees whose job duties require specialized access to IT resources (servers and/or databases).

5. Policy Statement. The Department shall manage all privilege access accounts per the principle of least privilege, including but not limited to being monitored and audited regularly, approved by the appropriate authority, and revoked when access is no longer applicable. Privileged access system users shall adhere to Department's confidentiality, integrity, and availability policies. Employees are responsible for information security and are subject to disciplinary actions, including dismissal and civil and criminal penalties for failure to adhere to the privileged access authorization protocols.

6. Privileged Access Authorization Process. Department staff must obtain permission from the appropriate approval authority before accessing Departmental IT Resources. Only Department staff whose job duties require access to support the Department's mission shall receive privileged access, which permits but is not limited to running jobs and services independent of user interaction.

6-1. Initiate Request. The Requestor (or designee) must submit privileged-level access requests via the DCF Statewide Help Desk ticketing system to the Department's Information Security Manager (ISM) for review and to obtain the appropriate approvals. The Requestor should include the following information in the ticket request:

a. Short Description. Privileged Access Authorization Request

b. Description. Within the description section, include the following information, if applicable:

(1) Job Title
(2) Department/Program Area Assigned
(3) Specify the Level of Access.
    (a) Read Only Rights
    (b) Read/Write Rights
    (c) Administrative Rights (Reserved for authorized/approved OITS staff)

(4) Indicate the Resource. The resource includes but is not limited to wireless local area network (WLAN), local area network (LAN), servers (on-premises/cloud), and cloud services platforms (dynamics, Azure Synapse, PowerBI, etc.); the Requestor requires privileged-level access.

    (a) Name
    (b) Location
    (c) Criticality and Data Classification

(5) Business Justification for the Request.

6-2. Approval Process. The ISM shall coordinate the review of each access request and determine if access is appropriate and necessary for the Requestor to perform their duties. The Requestor should receive status updates via the Department's ticketing system. If approved, the ISM shall notify the appropriate personnel.

6-3. Provision Process. When necessary, OITS staff shall notify third parties (i.e., State Data Center) via an authorized ticketing system process to grant the Requestor privilege-level access to Department IT Resources under the authority of the CIO.

6-4. Monitor. All Department IT resource users shall have no expectation of privacy in their use of DCF IT resources; such use constitutes consent to monitoring activities with or without staff knowledge. The Department reserves the right to deploy automated mechanisms when applicable to monitor the use and management of server-level access accounts. These mechanisms log account activity and generate notifications of atypical account usage based on the criticality of the server; refer to CFOP 50-2.

6-5. Access Management. The Department shall periodically review the privileged access granted to Department information systems, at minimum quarterly or whenever access is no longer needed, and make the appropriate updates. The Department shall modify, disable, or restrict privileged access to Department IT systems when abnormal behavior is detected or when job duties or role changes occur.

7. Delegation of Privileged Access. Privileged access can be delegated to other users only if the person delegating access has the authorization to do so. The recipient of the access must submit a DCF Statewide Help Desk ticket request to the ISM; in the 'short description' field, enter the following: 'Delegation of Privilege Access Authorization Request' and complete the applicable information per section 6-1 of this operating procedure.

8. Reporting Security Incidents. Staff shall report suspected inappropriate behavior or violation of Department access policies and procedures per CFOP 50-2, Chapter 3, *Event and Incident Reporting* SOP S-4, *CSIRT Operating Procedure*s.