STATE OF FLORIDA
DEPARTMENT OF CHILDREN AND FAMILIES
TALLAHASSEE, December 12, 2024

CF OPERATING PROCEDURE
NO. 50-3

System Management

# SECURITY PLANNING

This operating procedure establishes the Department of Children and Families (Department or DCF) standards for security planning across the Department's enterprise.

BY DIRECTION OF THE SECRETARY:

(Signed copy on file)

COLE SOUSA
Chief Information Officer

SUMMARY OF REVISED, DELETED, OR ADDED MATERIAL

Annual review completed and revisions made to the System Security Plan approval process to reflect current policies and procedures, including the Department's HIPAA Privacy and Security Officers. This operating procedure supersedes CFOP 50-3, dated June 13, 2022.

# Contents

1. Purpose ..... 3
2. Scope ..... 3
3. References ..... 3
4. Definitions ..... 3
5. Statement of Policy ..... 4
   a. System Security Plan ..... 4
   b. Artificial Intelligence (AI) ..... 6
      (1) Responsible ..... 6
      (2) Equitable ..... 6
      (3) Traceable ..... 6
      (4) Reliable ..... 6
      (5) Governable ..... 6
   c. Rules of Behavior ..... 6
   d. Security-Related Activity Planning ..... 7
   e. Security Concept of Operations ..... 8
   f. Information Security Architecture ..... 8
   g. Central Management ..... 8
6. Enforcement ..... 9
7. Review and Revise ..... 9

1. Purpose. This operating procedure establishes the minimum requirements for the Office of the Information Technology Services (OITS) when it comes to developing a system security plan.

2. Scope. This operating procedure applies to any information technology resources connecting to the Department's network, whether used in offices, remotely, or at telecommuting sites. All information technology resource users (department employees, contractors, vendors, or others) are responsible for adhering to this operating procedure.

3. References.

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

d. 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.

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

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

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

h. NIST AI 100-1, "Artificial Intelligence Risk Management Framework (AI RMF 1.0)."

4. Definitions.

a. Artificial Intelligence (AI). An engineered or machine-based system that can, for a given set of objectives, generate outputs such as predictions, recommendations, or decisions influencing real or virtual environments. AI systems are designed to operate with varying levels of autonomy.

b. Chief Information Officer (CIO). The Department executive who oversees the staff, processes and technologies within the Department's Office of Information Technology Services to ensure delivery of outcomes that support the goals of the Department's business in a manner consistent with the Department's Mission, Vision, and Values. The duties of the CIO include the management and oversight of all Department business applications in the OITS areas of Department program office support.

c. Confidential Information and/or Confidential Data. Information not subject to inspection by the public that may be released only to those persons and entities designated in Florida Statute; information designated as confidential under provisions of federal law or rule, including but not limited

to, Federal Tax Information (FTI), Protected Health Information (PHI), Personally Identifiable Information (PII), and drivers' license information and/or photographs.

d. Cybersecurity Resources. Data processing hardware (including desktop computers, laptops, tablets, smartphones and associated devices); software and services; supplies; personnel; facility resources; maintenance; and training or other related resources.

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.

f. Exempt Information. Information the department is not required to disclose under Section 119.07(1), F.S. or Section 282.318, F.S., but which the department is not necessarily prohibited from disclosing in all circumstances.

g. Information Security Manager (ISM). 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.

h. Security Concept of Operations (Security CONOP). This federal term is for a specific section of a System Security Plan and the security-focused description of a specific information system, its operational policies, classes of users, interactions between the system and its users, and that system's contribution to the operational mission.

5. Statement of Policy. OITS should plan and coordinate security-related activities affecting DCF applications as per the roles and responsibilities described below.

a. System Security Plan.

(1) In OITS, each Application Director or their delegated Manager should develop a system security plan (SSP) for their individual applications that describes the processes, procedures, and security requirements, and describes the security controls in place or planned for meeting those requirements. The SSP should be consistent with the guidance provided in NIST 800 SP 800-18, *Guide for Developing Security Plans*, and the security plan should adhere to the following requirements:

(a) Consistent with OITS's enterprise architecture.

(b) Explicitly defines the authorization boundary for the system.

(c) Describes the operational context of the application in terms of missions and business processes.

(d) Provides the security categorization of the application including supporting rationale.

(e) Describes the operational environment for the application.

1. All IT assets, including hardware, software, and (if appropriate) networking/telecommunication equipment, should be listed and described.

2. The description should reflect any environmental or technical factors that are of security significance (e.g., versions, protocols, ports, cloud and/or wireless technology, public access, hosting or operation at a facility outside of the organization's control), as applicable.

(f) Describes relationships with or connections to other information systems. The description should include applicable diagrams (e.g., network diagrams, system boundary, interconnections, data flow, and high-level design).

(g) Provides an overview of the security requirements for that specific system.

(h) Is completed based on the results of compliance requirements and risk assessment and describes how existing or planned security controls provide adequate mitigation of any identified risks to which the application is subject to.

(i) Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring and supplementation decisions and a schedule for implementing planned controls.

(j) Is reviewed and approved by the HIPAA Privacy Officer when applicable, including the ISM (also known as the HIPAA Security Officer), Deputy CIO, and CIO prior to plan implementation.

(2) OITS Application Directors should review any SSPs for the applications in their business unit every 365 days, or more often if necessary due to material change, and resubmit the SSP for approval per section 5.a(1)(j).

(3) OITS Application Directors or their delegated Managers should update their SSPs to address changes to their applications or the operational environment, in addition to addressing any issues identified during plan implementation or any security control assessments.

(a) SSPs should be updated when impacted by unforeseen significant events, such as a breach, a new threat, or previously unknown vulnerability.

(b) SSPs should be updated when there is a significant change to the system, including a change in the points of contact, system architecture, system status, system interconnections, or system scope.

(c) SSPs should be reviewed and revised to factor in planned application enhancements, to ensure that required security-related activities are planned for in advance.

(4) The respective OITS Application Director or delegated Manager should plan, document, and implement additional mitigating security controls for their application if the CIO does not approve their SSP, and then resubmit to the CIO for approval.

(5) The Director over each OITS application is responsible for verifying and validating compliance with the provisions of this operating procedure and should request assistance from the ISM and OITS Audit and Compliance Analyst as needed.

b. Artificial Intelligence (AI). When applicable, OITS shall align existing business practices and technology frameworks to advance the innovative use of artificial intelligence in Department-owned/leased IT resources. The Department's AI ethical principles encompass five significant areas; for additional details, refer to CF Pamphlet 50-3.1, Use of Generative Artificial Intelligence (Machine Learning):

(1) Responsible. Department employees shall exercise appropriate levels of judgment and care while remaining responsible for the developing, deploying, and using AI capabilities.

(2) Equitable. The Department shall take deliberate steps to minimize unintended bias in AI capabilities.

(3) Traceable. The Department shall develop and deploy AI capabilities so that relevant personnel understand the technology, development processes, and operational methods applicable to AI capabilities, including with transparent and auditable methodologies, data sources, design procedure, and documentation.

(4) Reliable. The Departments AI capabilities will have explicit, well-defined uses, and the safety, security, and effectiveness of such capabilities will be subject to testing and assurance within those defined uses across their entire life cycles.

(5) Governable. The Department shall design and engineer AI capabilities to fulfill their intended functions while possessing the ability to detect and avoid unintended consequences, and disengage or deactivate deployed systems that demonstrate unintended behavior.

c. Rules of Behavior.

(1) The OITS Application Director or delegated Manager or designee should:

(a) Establish and make readily available to all information system users, the rules that describe their responsibilities and expected behavior regarding information and information system usage.

(b) This set of rules should include general rules for all users and targeted rules for specific functions such as information system administration, developers, end users, etc.

(c) If the rules developed are not covered by existing written DCF Policies and Security Agreement forms, the OITS Application Director or delegated Manager is responsible for identifying and addressing any gaps and should request assistance from the ISM and/or the OITS Audit and Compliance Analyst as needed.

(2) OITS Application Director or delegated Manager should receive signed acknowledgment from users indicating that they have read, understand, and agree to abide by these rules before authorizing access to information and the application.

(a) Electronic signatures are acceptable for use in acknowledging these rules.

(b) Require individuals who have signed a previous version of the rules to read and re-sign whenever the rules for accessing the system are revised/updated.

(3) These rules should include explicit restrictions on the use of social networking sites, posting information on commercial websites, and sharing application account information.

(4) Additionally, these rules should include the following information:

(a) Users should store all data files and other critical information on a network share not on individual user endpoints.

(b) Users should store media (e.g., USB drives and external hard drives) in a secure location away from extreme temperature and sunlight.

(c) Users should report any apparent or actual resource violation to their supervisor for review as a possible security event.

(5) The Department ISM is responsible for documenting an acceptable use policy, consistent with NIST SP 800-53, which should prohibit users from misusing system resources in a manner consistent with SSP controls development.

d. Security-Related Activity Planning.

(1) The OITS Application Director or delegated Manager should plan and coordinate security-related activities affecting the application before conducting such activities in order to reduce the impact on organizational operations (i.e., mission, functions, image4, and reputation), organizational assets, and individuals.

(2) Organizational advanced planning and coordination includes both emergency and nonemergency (i.e., planned or non-urgent unplanned) situations.

(3) The OITS Application Director or delegated Manager should identify and coordinate with the stake holders and participants for each application and security-related activity. These persons include, but are not limited to, the following:

(a) Business process owners;

(b) Users;

(c) Security personnel;

(d) Operations support personnel; and,

(e) Appropriate personnel of connected systems.

NOTE: Security-related activities include, for example, security assessments, audits, system hardware and software maintenance, and contingency plan testing/exercises.

e. Security Concept of Operations.

(1) The term Security Concept of Operations (Security CONOPS) is a federal level term for a typically traditional section of an SSP. The Security CONOPS can be a text, graphic, or combination of both that communicates the characteristics of the business information system from the stakeholder's perspective (those who will use the system) and shows how these capabilities may be employed to achieve desired objectives. Ideally the Security CONOPS would be included in the SSP but could be included in another system document.

(2) The OITS Application Director or delegated Manager should:

(a) Develop a Security CONOPS for the application containing, at a minimum, how the organization intends to operate the system from the perspective of information security; and,

(b) Review and update the Security CONOPS as needed, at a minimum of every 365 days.

f. Information Security Architecture. The OITS Application Director or delegated Manager should:

(1) Develop an information security architecture for each application that:

(a) Describes the overall philosophy, requirements, and approach to be taken with regard to protecting the confidentiality, integrity, and availability of the organizational information in the application;

(b) Describes how the information security architecture is integrated into and supports the enterprise architecture of the application; and,

(c) Describes any information security assumptions about, and dependencies on, external services.

(2) Review and update the information security architecture as needed, with a minimum of every 365 days, to reflect updates in the enterprise architecture; and,

(3) Ensure that planned information security architecture changes are reflected in the SSP, the Security CONOPS, and organizational procurements/acquisitions.

g. Central Management. OITS centrally manages the security controls and related processes on its applications under the direction of the CIO. Central management over security controls and processes includes:

(1) Planning;

(2) Implementing;

(3) Assessing;

(4) Authorizing; and,

(5) Monitoring.

6. Enforcement. Violations of information security policies and procedures may result in loss or limitations on use of information technology resources, disciplinary action up to and including termination of employment or contractual relationship, and/or referral for civil or criminal prosecution as provided by law.

7. Review and Revise. This operating procedure will be reviewed as deemed appropriate, but no less frequently than every 365 days or when a significant change occurs, whichever occurs first. The review will be performed by the department's Information Security Manager.