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.**
   e. IRS Publication 1075, “Safeguards Program.”
   f. Title XIII, Section 13402, “Notification in the Case of Breach.”
   h. 26 U.S. Code § 6103, “Confidentiality and disclosure of returns and return information.”

4. **Definitions.**
   a. **Chief Application Owner (CAO).** The duties of the Chief Application Owner (CAO) span the management and oversight of all Department business applications in the OITS areas of Department program office support.

   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.

   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. **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.

e. **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.

f. **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 74-2, F.A.C.

g. **Information Technology 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.

h. **Security Concept of Operations (Security CONOP).** A security-focused description of an information system, its operational policies, classes of users, interactions between the system and its users, and the system’s contribution to the operational mission.

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

   a. **System Security Plan.**

      (1) In OITS, each Business Information System Director or delegated Manager should develop a system security plan (SSP) for their business information system 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 business information system in terms of missions and business processes.

         (d) Provides the security categorization of the business information system including supporting rationale.

         (e) Describes the operational environment for the business information system.

      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, 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 business information system is subject.

(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 ISM, CAO, and CIO prior to plan implementation.

(2) The OITS Business Information System Director or delegated Manager should review any security plans for the business information systems in their business unit every 365 days, or more often if necessary due to material change, and resubmit the SSP to the ISM, the CAO, and the CIO for approval.

(3) The OITS Business Information System Director or delegated Manager should update the plan to address changes to the business information system/environment of operation or problems identified during plan implementation or security control assessments.

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

(b) The SSP 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) The SSP should be updated to factor in planned business information system enhancements, to ensure that required security-related activities are planned for in advance.

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

(5) The Director over each OITS business information system is responsible for verifying and validating compliance with the provisions of this policy and should request assistance from the ISM and OITS Audit and Compliance Analyst as needed.
b. **Rules of Behavior (ROB).**

(1) The OITS Business Information System 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 with regard to information and information system usage.

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

   (c) If their expected ROB are not covered by existing written DCF Policies and Security Agreement forms, the OITS Business Information System Director or delegated Manager is responsible for addressing any gaps and should request assistance from the ISM and OITS Audit and Compliance Analyst as needed.

(2) OITS Business Information System Director or delegated Manager receive signed acknowledgment from users indicating that they have read, understand, and agree to abide by the ROB before authorizing access to information and the business information systems.

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

   (b) Require individuals who have signed a previous version of ROB to read and re-sign when the ROB is revised/updated.

(3) Include in the ROB explicit restrictions on the use of social networking sites, posting information on commercial websites, and sharing business information system account information.

(4) Include in the ROB the following information:

   (a) Users should store all data files and other critical information on a network share.

   (b) Users should store media (e.g., USB drives and CD-ROM discs) 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.

c. **Security-Related Activity Planning.**

(1) The OITS Business Information System Director or delegated Manager should plan and coordinate security-related activities affecting the business information system 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 Business Information System Director or delegated Manager should identify and coordinate with the stakeholders and participants for each business information system 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.


(1) The OITS Business Information System Director or delegated Manager should:

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

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

(2) The 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 CONOPS would be included in the SSP but may be included in another system document.

e. Information Security Architecture. The OITS Business Information System Director or delegated Manager should:

(1) Develop an information security architecture for each business information system 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 business information system;

(b) Describes how the information security architecture is integrated into and supports the enterprise architecture of the business information system; 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.
f. Central Management. OITS centrally manages the security controls and related processes on its business information systems. 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 Revision. This operating procedure will be reviewed as deemed appropriate, but no less frequently than every 365 days. The review will be performed by the department's Information Security Manager.

BY DIRECTION OF THE SECRETARY:

(Signed original copy on file)

JOE VASTOLA
Chief Information Officer

<table>
<thead>
<tr>
<th>SUMMARY OF REVISED, Deleted, Or Added Material</th>
</tr>
</thead>
<tbody>
<tr>
<td>New operating procedure to meet IRS, SSA, and MARS-E 2.0 compliance requirements.</td>
</tr>
</tbody>
</table>