STATE OF FLORIDA
DEPARTMENT OF
CHILDREN AND FAMILIES
TALLAHASSEE, October 6, 2022

CF OPERATING PROCEDURE
NO. 50-27

Systems Management

DATA CLASSIFICATION AND ACCESS CONTROL

1. Purpose. This operating procedure implements section 282.318, Florida Statutes (F.S.), Chapter 60GG-2, Florida Administrative Code (F.A.C.) by describing the standards for compliance with both state and federal information security control frameworks.

a. Data classification is the first step toward identifying how Department data and information should be protected based on Department policies and applicable state and federal laws. Data classification provides the knowledge necessary for staff and leadership to apply the most cost effective and appropriate level of protection as part of a risk-based approach to security and privacy access controls implementation.

b. Data classification supports compliance with legal and regulatory requirements, mapping data protection levels to organizational needs, and supports efficient budgeting by implementing controls where they are needed the most, all while reducing risks associated with the unauthorized access and disclosure of Department confidential or restricted data.

c. All DCF data and information, regardless of the format or medium of the record (paper, electronic data/voice/video/image, microfilm, etc.), should be classified into one of three sensitivity level categories:

(1) Level 1 – Restricted.

(2) Level 2 – Confidential.

(3) Level 3 – Public.

2. Scope. This operating procedure covers all Department employees who come in contact with sensitive DCF internal information. All information technology resource users (Department employees, contractors, vendors, or others) are responsible for adhering to this operating procedure.

a. Sensitive information is either confidential or restricted information, and both are defined in paragraph 4 of this operating procedure.

b. Although this operating procedure provides overall guidance to achieve consistent information protection, Office of Information Technology Services (OITS) employees are expected to apply and extend these concepts to fit the needs of day-to-day of information and business systems operations.

c. The OITS data classification process, as defined in this operating procedure, is based on the concepts of need-to-know and “least privilege.” These terms mean that Department information is not disclosed to any person who does not have a legitimate and demonstrable business need to receive that information. Operationalization of these concepts, when combined with the policies defined in this operating procedure, contribute toward protecting Department information from unauthorized disclosure, use, modification, and deletion.

d. This data classification procedure is applicable to all electronic information for which OITS is the custodian.

3. References.

a. Section 282.318, F. S., *State Cybersecurity Act.*

b. Section 501.171, F. S., *Security of Confidential and Personal Information*.

c. Rule Chapter 60GG-2, F.A.C., *Florida Cybersecurity Standards*.

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

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. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Rev. 5, *Security and Privacy Controls for Information Systems and Organizations*.

i. NIST SP 800-60 Vol.2 Rev. 1, *Guide for Mapping Types of Information and Information Systems to Security Categories: Appendices*.

j. Federal Information Processing Standard (FIPS) Publication 199, Standards for Security Categorization of Federal Information and Information Systems (2021).

k. Title III of the E-Government Act, titled the Federal Information Security Management Act (FISMA) of 2002.

l. Federal Information Security Modernization Act (FISMA) of 2014 (Public Law 113-283; December 18, 2014).

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

a. 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 statutes; 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.

b. 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 contracted by the department who have access to department IT resources.

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

d. Information Custodians. Agency information technology workers who maintain or administer information resources on behalf of information owners. A person or team that holds the day-to-day responsibility for information technology infrastructure resources. An Information Custodian may also be referred to as Data Custodian.

e. Information Owner. The manager of the business unit ultimately responsible for the collection, maintenance, and dissemination of a specific collection of information or business information system.

f. Information Security Manger. The Information Security Manager (ISM) is the person designated by the Secretary of the Department to report to the Chief Information Officer (CIO) and administer the Department's information technology security program, supporting all ongoing activities that serve to protect the confidentiality and integrity of information in compliance with Department and statewide policies and standards in accordance with section 282.318, F.S., and Chapter 60GG-2, F.A.C.

5. Access Control Procedures.

a. Access Granting Decisions. Access to Department sensitive information must be provided only after the documented authorization of the Information Owner has been obtained.

(1) Access requests will be presented to the Information Owner, or their designated staff, using the appropriate Access Request form or electronic form.

(2) Information Custodians must refer all requests for access to a department business system to the relevant Information Owner or their delegates and may not grant access without the knowledge and approval of the Information Owner.

(3) Special needs for other access privileges will be dealt with by the Information Owner on a request-by-request basis.

(4) The list of individuals with access to confidential or restricted data must be reviewed for accuracy by the relevant Information Owner, or their designated staff, in accordance with a system review schedule consistent and compliant with state and federal laws. The system review schedule must be approved by the Information Owner.

b. Need To Know. Each of the requirements set forth in this operating procedure are based on the concept of need to know and the principal of least privilege. If an OITS employee is unclear how the requirements set forth in this operating procedure should be applied to any particular circumstance, he or she must conservatively apply the need to know concept and confer with their supervisor for guidance. Information must be disclosed only to those employees who have a legitimate business need for the information.

c. System Access Controls. The proper controls shall be in place to authenticate the identity of users and to validate each user’s authorization before allowing the user to access information or services on any DCF business system.

(1) Data used for authentication shall be protected from unauthorized access.

(2) Controls shall be in place to ensure that only personnel with the proper authorization and a need to know are granted access to DCF systems and their resources.

(3) Remote access shall be controlled through secure identification and authentication mechanisms.

6. Information Classification Procedures.

a. Owners and Production Information. All electronic information owned by Department and managed by OITS must have a designated Information Owner.

(1) Production information is information routinely used to accomplish business objectives. Owners should be at the level of Director or above.

(2) Information Owners are responsible for assigning one of the three appropriate sensitivity classifications as defined below. Department Information Owners do not legally own the information entrusted to their care, instead they are designated members of the Department's management team who act as stewards, supervising the ways in which certain types of information are used and protected.

(a) Restricted (Level 1). This classification applies to the most sensitive business information that is intended for use strictly within DCF. Its unauthorized disclosure could seriously and adversely impact DCF, its customers, its business partners, and its vendors.

(b) Confidential (Level 2). This classification applies to less-sensitive business information that is intended for use within DCF. Its unauthorized disclosure could adversely impact DCF or its customers, vendors, business partners, or employees.

(c) Public (Level 3). This classification applies to information that has been approved by Department management for release to the public. By definition, there is no such thing as unauthorized disclosure of this type of information, and it may be disseminated via Department without potential harm.

b. Owners and Access Decisions. Information Owners must make decisions about who will be permitted to gain access to information, and the uses to which this information will be put. OITS must take steps to ensure that appropriate controls are utilized in the storage, handling, distribution, and regular usage of electronic information.

7. Object Reuse and Disposal Procedures.

a. If storage media is being reallocated, care should be taken to ensure that residual data cannot be recovered or accessed by unauthorized users.

b. Simply deleting the data from the media is not sufficient, it must be sanitized ("wiped"). As per Department policy, all storage media shall be completely wiped before reassigning that medium to a different user or disposing of it when no longer used.

c. A method must be used that completely erases all data. Department data sanitization processes currently involve following the methods detailed in Department of Defense (DoD) 5220.22-M, the National Industrial Security Program Operating Manual, or NIST SP 800-88, Guidelines for Media Sanitization. These methods involve overwriting all data tracks at a minimum of three times, depending on risk level.

d. When disposing of electronic storage media containing data that cannot be completely erased, the media must be destroyed in a manner approved by the Department's ISM, CIO, and the Information Owner for the respective business system. Storage media containing sensitive (i.e., restricted or confidential) information must always be escorted by the Information Owner or their delegate if it leaves the Department for destruction, and the Information Owner or delegate must witness and document the destruction of the media.

8. Physical Security Procedures (Facility Access) (also see CFOP 50-2). All network equipment (routers, switches, etc.) and servers located at Headquarters and located in regional facilities must be secured when no Department personnel, or authorized contractors, are present. Physically secured is defined as locked in a location that denies access to unauthorized personnel.

9. Special Procedures for Restricted Information (also see CFOP 50-2). If restricted information is going to be stored on a personal computer, portable computer, tablet, smartphone, or any other single-user system, the system must conform to data access control safeguards approved by OITS and the Department ISM. When these users are not currently accessing or otherwise actively using the restricted information on such a machine, they must not leave the machine without logging off, invoking a password protected screen saver, or otherwise restricting access to the restricted information.

10. Data Encryption Software Procedures. Department employees and vendors must not install non-standard encryption software to encrypt files or folders without the express written consent of both the Information Owner for whom they are working and by the Department's CIO.

11. Information Transfer Procedures.

a. Transmission over Networks. If Department restricted data is to be transmitted over any external communication network, it must be sent only in encrypted form. Such networks include electronic mail systems, the Internet, etc. All such transmissions must use a virtual private network (VPN) or similar software as approved by the Information Owner and OITS.

b. Transfer to Another Computer. Before any restricted information may be transferred from one computer to another, the person making the transfer must ensure that access controls on the destination computer are commensurate with access controls on the originating computer. If comparable security cannot be provided with the destination system's access controls, then the information must not be transferred.

12. Software Security Procedures (also see CFOP 50-2).

a. Secure Storage of Object and Source Code. At DCF, the business application teams use a source code configuration management tool that provides controlled access to separate the roles of development, testing, and production by functionality.

(1) Object and source code for system software shall always be securely stored when not in use by the developer.

(2) Developers must not have access to modify program files that actually run in production.

(3) Changes made by developers must be implemented into production by technical operations.

(4) Unless access is routed through an application interface, no developer shall have more than read access to production data. Further, any changes to production applications must follow the department's change management process.

b. Testing. At DCF, the business application teams use a workflow automation tool to track through the testing process toward change management for final review and release scheduling. Developers must at least perform functional testing. Final testing must be performed or managed by the quality implementation and controls staff working with the User Acceptance Testing team toward promotion into production.

c. Backups. Sensitive data shall be backed up regularly, and the backup media shall be stored in a secure environment.

13. Key Management Procedures.

a. Protection of Keys. Public and private keys shall be protected against unauthorized modification and substitution.

b. Generation, Handling, Disposal and Destruction. Procedures shall be in place to ensure proper generation, handling, and disposal of keys as well as the destruction of outdated keying material.

c. Safeguarding of Keys. Procedures shall be in place to safeguard all cryptographic material, including certificates. OITS Operational Security must retain custody of keys or copies of keys for safekeeping.

14. Enforcement Procedures. Violations of information security policies and procedures may result in loss or limitations on use of information resources, disciplinary action, up to and including separation from employment at the department, an end to employment or contractual relationship, and referral for civil or criminal prosecution as provided by law.

15. Review Procedures. This operating procedure will be reviewed as deemed appropriate, but no less frequently than every 365 days. This review, and, if needed, updating, will be performed by the ISM under the guidance of the CIO.

BY DIRECTION OF THE SECRETARY:

(Signed original copy on file)

COLE SOUSA
Chief Information Officer

SUMMARY OF REVISED, DELETED, OR ADDED MATERIAL

Annual review and revision completed; no substantive changes.