State of Florida
AGENCY FOR HEALTH CARE ADMINISTRATION

POLICY/PROCEDURE NUMBER: **4004**
SUBJECT: **Records Management**
DIVISION: **Operations**
BUREAU: **Support Services**
SECTION: **Records Management**

1.0 PURPOSE/SCOPE

The purpose of this policy is to provide uniform procedures for the Agency's Records Management Program. The Records Management Program exists to ensure records are maintained as appropriate, so that information is available when and where it is needed. This policy applies to all Agency employees, including OPS and contracted staff, and all Agency records regardless of the medium in which they exist.

2.0 AUTHORITY

- Chapter 119, Florida Statutes (F.S.), Public Records
- Chapter 257, F.S., Public Libraries and State Archives
- Chapter 282, F.S., Communications and Data Processing
- Chapter 501.171, F.S., Security of Confidential Personal Information
- Chapter 1B-11.004, Florida Administrative Code (F.A.C.), Use of Archives
- Chapter 1B-24, F.A.C., Public Records Scheduling and Disposition
- Chapter 1B-26, F.A.C., Records Management – Standards and Requirements
- Federal Information Processing Standards Publication Secure Hash Standards
- The Unicode Standard

3.0 DEFINITIONS

Accession - Transfer of records into the physical custody of the Department of State's State Record Center (SRC).

Active Records - Records that still have sufficient administrative, fiscal, legal, or historical value to warrant their continued storage in an easily accessible area (e.g., office area).

Archives - Inactive records which have been determined to have long term use due to their historical value.

Confidential Records - Records that the Agency is legally prohibited from making available for inspection or copying.

Disposition - Destruction of inactive records that have met their retention period.

Database - Organized collection of automated information. Chapter 1B-26.003, F.A.C. sets the standards and requirements for databases.

Database Management Systems - A set of software programs that controls the organization, storage, and retrieval of data (fields, records and files) in a database. Chapter 1B-26.003, F.A.C. sets the standards and requirements for database management systems.

DRD – The Disposition Records Document is a form used by the Department of State to request approval from the Agency to dispose of records that have met their retention schedule.

Electronic Storage - Numeric, graphic, and textual information which may be recorded in any machine readable media form which includes, but is not limited to, magnetic media, such as tapes, disks and flash drives.

Electronic Records – Any information that is recorded in machine readable form.

E-mail (Electronic Message) - A method of transmitting information that must be evaluated just like information received through mail, fax, or in person.

Exempt Records - Public records specifically exempted by law from public inspection and copying, although they may still be able to be released to the public by the Agency.

Inactive Record - Records which have lost some of their value or have been superseded by new records, but are not yet ripe for destruction. Records that are referenced less than once per month are considered inactive.

Micrographics - Area of records management associated with the feasibility, production, handling, care, and use of records which have been photographically copied and reduced in size to preserve information or reduce storage space.

Protected Health Information (PHI) - Any information, including demographic information, which relates to: the individual's past, present, or future physical or mental health or condition, the provision of health care to the individual, or the past, present, or future payment for the provision of health care to the individual, and that identifies the individual or for which there is a reasonable basis to believe can be used to identify the individual. Protected health information includes many common identifiers (e.g., name, address, birth date, Social Security Number) when they can be associated with the health information listed above.

Public Record - Section 119.011(12), F.S., defines public records as all documents, papers, letters, maps, books, tapes, photographs, films, sound recordings, data processing software, or other material, regardless of physical form, characteristics, or means of transmission, made or received pursuant to law or ordinance or in connection with the transaction of official business by any agency.

RDD – The Records Disposition Document is a form used by the Agency for records that have been stored within Agency offices and are not sent to the State Records Center for storage or disposal. The form is used to record the destruction of eligible records.

Records Custodian - Supervisor or manager in a division or bureau who has oversight authority of the records in his/her control.

Records Management Coordinator - Person designated within each Agency bureau to coordinate records management, including responses to public records requests.

Records Management Liaison Officer (RMLO) - Employee within the Bureau of Support Services assigned the responsibility of record management and quality control of records for the Agency.

Record Series – Chapter 1B-24.001(3)(k), F.A.C. defines record series as a group of related public records arranged under a single filing arrangement or kept together as a unit (physically or intellectually) because they consist of the same form, relate to the same subject or function, result from the same activity, document a specific type of transaction, or have some other relationship arising from their creation, receipt, or use. A record series might contain records in a variety of forms and formats that document a particular program, function, or activity of the agency.

Retention Schedule - Period of time in which record series are required to be retained before being scheduled for disposal.

State Records Center - Records storage facility located in Tallahassee operated by the Department of State. Also known as the SRC.

Total Recall - A web-based system which allows the user to perform certain records management functions, such as ordering supplies, accessioning items, etc., online through a secure, user specific login.

4.0 POLICY

It is the Agency's policy to ensure that public records in its custody are maintained and managed as required by Florida Public Records Law, including appropriate retention, release, and disposition. Florida Public Records Law provides that all materials made or received by Florida's state and local government agencies in connection with their official business are public records. Records may not be withheld unless the record is specifically designated under law as confidential or exempt from public disclosure.

5.0 PROCEDURES

I. Areas of Responsibility

A. The Agency has appointed a RMLO within the Bureau of Support Services. The RMLO will:

1. Ensure that all divisions comply with the requirements and procedures outlined in this policy and procedure.

2. Provide liaison between Agency Records Custodians and Coordinators and the Department of State.

3. Assist Agency staff with preparing records retention schedules, preparing records for archiving, and other records management tasks.

4. Disseminate destruction requests from the SRC as records are determined to be eligible for destruction and then submit the completed forms back to the SRC.

B. Each Bureau Chief or equivalent shall serve as the Records Custodian for all records created or received by his/her respective bureau/unit. These duties may be delegated at the discretion of the Bureau Chief, however, the Bureau Chief or equivalent retains responsibility for these records. Each Records Custodian shall:

1. Ensure security of records physically stored at his/her location;

2. Ensure proper destruction of records which have met their retention schedule and return all Disposal Request Documents (DRDs) to the Bureau of Support Services within fifteen (15) business days of receipt;

3. Ensure appropriate response to all public records requests received by his/her bureau/unit.

C. Each Bureau Chief or equivalent may also designate a Records Coordinator for his/her bureau/unit. The Records Coordinator shall:

1. Work with the RMLO to develop retention schedules as necessary;

2. Ensure that inactive records are removed from the active records inventory frequently;

3. Provide liaison between the RMLO and the Records Custodian;

4. Inform staff on changes/updates to the Agency Records Management Program;

5. Secure Records Custodian signature on DRDs for records that have met their retention schedule.

II. Records Management

A. Records management entails organization, maintenance, retention, storage, and disposition of public records.

1. Public records shall be organized, arranged, and maintained using a filing or records-keeping system that:

a. is appropriate to the nature, purpose, and use of the records;
b. can be easily understood by all users, and;
c. will facilitate the location of and access to those records, when and where it is needed.

B. Records Retention Schedules must be established for all records created and maintained by the Agency. Many of the Agency's records are covered by the General Records Schedule GS1-SL for Florida's State and Local Government Agencies (GS1-SL).

C. Any records not covered by the GS1-SL must have an individual schedule established. To establish an individual records retention schedule, contact the RMLO.

D. A link to the GS1-SL is maintained on the Bureau of Support Services' Records Management webpage.

E. Each bureau must systematically dispose of public records that have met their retention requirements and are no longer needed.

III. Inactive Records Storage (Archiving)

A. Once a record has lost its value as part of regular office operation, it is considered to be inactive. However, such records cannot be destroyed until their retention requirements have been met.

B. Inactive records may be retained in-house, imaged and stored electronically or stored in the SRC.

C. The SRC should be used to store inactive records whenever possible. If the records must be maintained in-house, they should be imaged and stored electronically if possible.

IV. Electronic Records

A. Records created or maintained in electronic format must be retained in accordance with the General Records Schedule GS1-SL (Section VI) regardless of whether the electronic records are the record copy or duplicates. A link to the GS1-SL is maintained on the Bureau of Support Services' Records Management webpage.

B. The Division of Information Technology will automatically save all non-spam filtered e-mail in archive for a period of seven (7) years. Any emails that are required to be maintained beyond that time period shall be maintained by the unit that created or received them.

C. The Agency shall develop and maintain adequate and up-to-date technical and descriptive documentation for each electronic recordkeeping system to specify characteristics necessary for reading or processing the records. The minimum documentation required is:

1. A narrative description of the system, including all inputs and outputs of the system; the organization and contents of the files and records; policies on access and use; security controls; purpose and function of the system; update cycles or conditions and rules for adding information to the system, changing information in it, or deleting information; and the location and

media in which electronic records are maintained and their retention requirements to ensure appropriate disposition of records in accordance with Chapter 1B-24, F.A.C.

2. The physical and technical characteristics of the records or the equivalent information associated with a database management system including a description of the relationship between data elements in databases.

3. For information coming from geographic information systems, the physical and technical characteristics of the records must be described in a description of the graphic data structure, such as recommended by the federal Spatial Data Transfer Standards.

4. Any other technical information needed to read or process the records.

D. Electronic recordkeeping systems used by the Agency that maintain record (master) copies of public records on electronic media shall meet the following minimum requirements:

1. Provide a method for all authorized users of the system to retrieve desired records.

2. Provide an appropriate level of security to ensure the integrity of the records, in accordance with the requirements of Chapter 282, F.S.

3. Security controls should include, at a minimum, physical and logical access controls, backup and recovery procedures, and training for custodians and users.

4. Automated methods for integrity checking should be incorporated in all systems that generate and use official file copies of records. Hashing algorithms and digital signatures should be considered for all official file copies of electronic records. The use of automated integrity controls, such as hashing algorithms and digital signatures, can reduce the need for other security controls. Hashing algorithms used to protect the integrity of official file copies of records should meet the requirements of Federal Information Processing Standards Publication 180-4 (FIPS-PUB 180-4) entitled "Secure Hash Standard". Agencies utilizing hashing algorithms shall only use validated implementations of hashing algorithms.

5. Identify the open format or standard interchange format when necessary to permit the exchange of records on electronic media between Agency electronic recordkeeping systems using different software/operating systems and the conversion or migration of records on electronic media from one system to another. For text records in the absence of other conversion capabilities, the word processing or text creation system should be able to import and export files in the ASCII or Unicode format as prescribed by the Unicode 5.0 Standard (or successor Unicode Standard).

6. Provide for the disposition of the records including, when appropriate, transfer to the SRC.

7. E-mail is not an appropriate storage media for documents to be retained. If a document requires retention, the document should be saved from e-mail to an approved format and system for retention. (For example Laserfiche or Sharepoint).

8. See also Email Retention Policy 5004.

V. Records Destruction

A. Records stored at the State Records Center

1. Twice a year the Department of State provides the RMLO with a list of documents, which have met their retention requirements and are eligible for destruction.

2. The RMLO will distribute the Disposition Request Documents (DRDs) to the appropriate Records Custodian for signature.

3. Unless the records are related to pending litigation, the DRDs should be signed and returned to the Agency RMLO for processing within fifteen (15) business days of receipt.

4. The RMLO will return the DRDs to the Department of State, and then the records will be destroyed.

B. Records stored within Agency Facilities

1. Identify records which have met their retention requirements and are eligible for destruction.

2. The completed Records Disposition Documents (RDDs) should be signed and returned to the Agency RMLO.

3. Identify documents that contain, or may contain confidential information or Protected Health Information (PHI) that are ready for disposal.

4. Place the identified documents in a locked shred bin.

5. If a locked shred bin is not available, or they are full, store the PHI in a locking file cabinet or a locking office until such time as an empty locked shred bin is available. Locking, rolling shred bins may also be available from your field office shredding contractor to handle overflow situations.

6. Never place PHI in regular trash or recycle bins – it must always be shredded.

7. If you are aware of PHI having been placed in regular trash, retrieve the PHI and properly dispose of it by shredding or placing it in a locked shred bin. If it is not possible to retrieve the PHI (for example, it has made it all the way to a dumpster), secure the trash receptacle/dumpster by posting staff near it to

deter access/emptying. Immediately, by direct telephone contact, contact the Agency HIPAA Privacy Officer and the facility management representative.

8. If you are unsure that something is, or contains PHI, shred it.

C. Records stored electronically

Electronic records may be destroyed only in accordance with the provision of Chapter 1B-24, F.A.C. Minimum standards are described in Chapter 1B-26.003, F.A.C. The Agency's Information Technology (IT) policy on media destruction (#08-IT-05) and Agency HIPAA policy (#4031), also discuss destruction of confidential electronic records.

In accordance with Section 501.171 (8), F.S., enacted in 2014, the Agency qualifies as a covered entity. The requirements from Section 501.171, F.S., is as follows: (8) REQUIREMENTS FOR DISPOSAL OF CUSTOMER RECORDS.—Each covered entity or third-party agent shall take all reasonable measures to dispose, or arrange for the disposal, of customer records containing personal information within its custody or control when the records are no longer to be retained. Such disposal shall involve shredding, erasing, or otherwise modifying the personal information in the records to make it unreadable or undecipherable through any means.

6.0 RESPONSIBILITIES

It is the responsibility of each Agency employee and contracted vendor to comply with this policy and procedure.

7.0 ENFORCEMENT

Violations of this policy may result in disciplinary action up to and including dismissal, in accordance with Rule Chapter 60L-36, Florida Administrative Code and Agency Policy Number 96-HR-33, Disciplinary Actions.

8.0 REVISION HISTORY

Author: Brian Kenyon **Date:** October 1, 2014

Approved by: Tonya Kidd **Date:** November 3, 2014

1st Revision Approved by: Tonya Kidd **Date:** January 20, 2016

2nd Revision Approved by: Jon Manalo **Date:** June 14, 2019

Deletion Approved by: _____ **Date:** _____

9.0 ATTACHMENT(S)