

CHAPTER 1B-26.003 RECORDS MANAGEMENT - STANDARDS AND REQUIREMENTS – ELECTRONIC RECORDKEEPING

(1) **PURPOSE.** These rules provide standards for record (master) copies of public records which reside in electronic recordkeeping systems. Recordkeeping requirements must be incorporated in the design and implementation of new systems and enhancements to existing systems. Public records are those as defined by Section 119.011(11), F.S.

(2) **AUTHORITY.** The authority for the establishment of these rules is Sections 257.36(1) and (6)(c), F.S.

(3) **SCOPE.**

(a)1. These rules are applicable to all agencies as defined by Section 119.011(2), F.S.

2. These rules establish minimum requirements for the creation, utilization, maintenance, retention, preservation, storage and disposition of record (master) copies, regardless of the media.

3. Electronic records include numeric, graphic, sound, video, and textual information which is recorded or transmitted in analog or digital form.

4. These rules apply to all electronic recordkeeping systems, including, but not limited to, microcomputers, minicomputers, main-frame computers, and image recording systems (regardless of storage media) in network or stand-alone configurations.

(b) Before existing records are committed to an electronic recordkeeping system, the agency shall conduct a cost benefit analysis to insure that the project or system contemplated is cost effective.

(c) Any electronic recordkeeping system not meeting the provisions of these rules may be utilized for long-term or permanent records provided the record (master) copy is maintained or microfilmed in accordance with the provisions of Rule 1B-26.0021, F.A.C., prior to disposition.

(4) **INTENT.** Electronic recordkeeping systems in use at the effective date of this rule, that are not in compliance with the requirements of this rule, may be used until the systems are replaced or upgraded. New and upgraded electronic recordkeeping systems created after the effective date of this rule shall comply with the requirements contained herein. The Department is aware that it may not be possible to implement this rule in its entirety immediately upon its enactment, and it is not the intent by this rule to disrupt existing recordkeeping practices provided that agencies make no further disposition of public records without approval of the Division of Library and Information Services of the Department of State.

(5) **DEFINITIONS.** For the purpose of these rules:

(a) "Database" means an organized collection of automated information.

(b) "Database management system" means a set of software programs that controls the organization, storage and retrieval of data (fields, records and files) in a database. It also controls the security and integrity of the database.

(c) "Data file" means related numeric, textual, sound, video, or graphic information that is organized in a prescribed form and format.

(d) "Electronic record" means any information that is recorded in machine readable form.

(e) "Electronic recordkeeping system" means an automated information system for the organized collection, processing, transmission, and dissemination of information in accordance with defined procedures.

(f) "System design" means the design of the nature and content of input, files, procedures, and output and their interrelationships.

(g) "Permanent or Long-term records" means any public records which have an established retention period of more than 10 years. See Section 119.011(11), F.S., for the definition of a public record.

(h) "Record (master) copy" means public records specifically designated by the custodian as the official record.

(i) "Geographic information system" means a computer system for capturing, storing, checking, integrating, manipulating, analyzing and displaying data related to positions on the Earth's surface.

(j) "Open format" means a data format that is defined in complete detail and that allows transformation of the data to other formats without loss of information. An open format may be either standards-based or proprietary.

(6) **AGENCY DUTIES AND RESPONSIBILITIES.** The head of each agency shall:

(a) Develop and implement a program for the management of electronic records.

(b) Ensure that all records are included within records retention schedules, either by being included within an applicable General Records Schedule, or by developing and obtaining approval for a

specific records retention schedule. Each record series shall be considered on an individual basis by the Division of Library and Information Services in establishing this retention period. See subsection 1B-24.001(3), F.A.C., for the definition of a record series.

(c) Integrate the management of electronic records with other records and information resources management programs of the agency.

(d) Incorporate electronic records management objectives, responsibilities, and authorities in pertinent agency directives, or rules, as applicable.

(e) Establish procedures for addressing records management requirements, including recordkeeping requirements and disposition, before approving, recommending, adopting, or implementing new electronic recordkeeping systems or enhancements to existing systems.

(f) Provide training for users of electronic recordkeeping systems in the operation, care, and handling of the equipment, software, and media used in the system.

(g) Ensure that electronic recordkeeping systems meet state requirements for public access to records.

1. STANDARD. Each agency which maintains public records in an electronic recordkeeping system shall provide, to any person making a request pursuant to Chapter 119, F.S., a copy of any data in such records which is not specifically exempt. Said copy shall be on paper, disk, tape, optical disk, or any other electronic storage device or media requested by the person, if the agency currently maintains the record in that form, or as otherwise required by Chapter 119, F.S. Except as otherwise provided by state statute, the cost for providing a copy of such data shall be in accordance with the provisions of Sections 119.07(4), F.S.

2. STANDARD. Except as otherwise provided by law, no agency shall enter into a contract with, or otherwise obligate itself to, any person or entity if such contract or obligation impairs the right of the public under state law to inspect or copy the agency's nonexempt public records existing on-line in, or stored on a device or media used in connection with, a computer system or optical imaging system owned, leased or otherwise used by an agency in the course of its governmental functions.

3. STANDARD. Each agency shall ensure that current and proposed electronic recordkeeping systems adequately provide for the rights of the public to access public records under Chapter 119, F.S.

4. STANDARD. In addition to ensuring that electronic recordkeeping systems meet requirements for public access to public records, agencies shall ensure that procedures and controls maintain confidentiality for information which is exempt from public disclosure.

(h) Develop and maintain documentation about electronic recordkeeping systems used by the agency to specify technical characteristics necessary for reading or processing the records. Documentation for electronic records systems shall meet the following standards:

1. STANDARD. Each agency shall identify all inputs and outputs of the system; define the organization and contents of the files and records; define policies on access and use; define the purpose and function of the system; define update cycles or conditions and rules for adding information to the system, changing information in it, or deleting information; and ensure the timely, authorized disposition of the records in accordance with Chapter 1B-24, F.A.C.

2. STANDARD. Each agency shall specify the location and media in which electronic records are maintained to meet retention requirements, establish and document security controls for the protection of the records, and maintain inventories of electronic recordkeeping systems to facilitate disposition.

(7) DOCUMENTATION STANDARDS.

(a) STANDARD. Agencies shall maintain adequate and up-to-date technical documentation for each electronic recordkeeping system. Documentation for electronic records systems shall be maintained in printed form, and should also be maintained in computer-readable form to facilitate access to the records. The minimum documentation required is:

1. A narrative description of the system;

2. The physical and technical characteristics of the records, including a record layout or markup language that describes each file or field including its name, size, starting or relative position, and description of the form of the data (such as alphabetic, decimal, or numeric), or a data dictionary 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 including a data dictionary, a quality and accuracy report

and a description of the graphic data structure, such as recommended by the federal Spatial Data Transfer Standards; and

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

(8) CREATION AND USE OF ELECTRONIC RECORDS AS RECORD (MASTER) COPIES. Electronic recordkeeping systems that maintain record (master) copies of public records on electronic media shall meet the following minimum requirements:

(a)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. Security controls should include, at a minimum, physical and logical access controls, backup and recovery procedures, and training for custodians and users. 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 US Federal Information Processing Standard Publication 180-1 (FIPS-PUB 180-1) (April 17, 1995) entitled "Secure Hash Standard," which is hereby incorporated by reference, and made a part of this rule. This publication is available from the National Technical Information Service (NTIS), 5285 Port Royal Road, U.S. Department of Commerce, Springfield, VA 22161, and at the Internet Uniform Resource Locator:

<http://www.itl.nist.gov/fipspubs/fip180-1.htm>. Agencies should also consider using only validated implementations of hashing algorithms in cases where the data being protected are of great intrinsic value or where the content and authenticity of the records are likely to be at issue in litigation.

3. 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 format as prescribed by Federal Information Processing Standard Publication (FIPS PUB) Number 1-2; entitled Coded Character Sets – 7-Bit American National Standard Code for Information Exchange (7-Bit ASCII) (1986, R2002), which is hereby incorporated by reference, and made a part of this rule. This publication is available from the National Technical Information Service (NTIS), 5285 Port Royal Road, U.S. Department of Commerce, Springfield, VA 22161; and

4. Provide for the disposition of the records including, when appropriate, transfer to the Florida State Archives.

(b) STANDARD. Before a record (master) copy is created on an electronic recordkeeping system, the record shall be uniquely identified to enable authorized personnel to retrieve, protect, and carry out the disposition of records in the system. Agencies shall ensure that records maintained in such systems can be correlated with any existing related records on paper, microfilm, or other media.

(9) LEGAL AUTHENTICATION. Agencies shall implement the following procedures to enhance the legal admissibility of electronic records:

(a) Document that similar kinds of records generated and stored electronically are created by the same processes each time and have a standardized retrieval approach.

(b) Substantiate that security procedures prevent unauthorized addition, modification, or deletion of a record and ensure systems protection against such problems as power interruptions.

(c) Identify the electronic media on which records are stored throughout their life cycle, the maximum time span that records remain on each storage media, and the official retention requirements as approved by the Division of Library and Information Services.

(d) State agencies shall, and other agencies are encouraged to, establish and maintain integrity controls for record (master) copies of electronic records in accordance with the requirements of Chapter 282, F.S.

(10) SELECTION OF ELECTRONIC RECORDS STORAGE MEDIA. For storing record (master) copies of electronic public records throughout their life cycle, agencies shall select appropriate media and systems which meet the following requirements:

(a) Permit easy and accurate retrieval in a timely fashion;

(b) Retain the records in a usable format until their authorized disposition and, when appropriate, meet the requirements necessary for transfer to the Florida State Archives.

(c) Obtain recording media only from vendors whose guarantee of 10 years or more of readability is based upon documented accelerated aging tests which are linked to specific locations on the media.

(d) STANDARD. A scanning density with a minimum of 300 dots per inch is required for recording electronic records.

(e) STANDARD. Record (master) copies of digital images must be stored in accordance with the TIFF 6.0 specification (June 3, 1992), which is hereby incorporated by reference and made a part of this rule. This specification is available from the Aldus Corporation, 411 First Avenue South, Seattle, WA 98104-2871. If use of a proprietary image format is unavoidable, the agency must provide a gateway to lossless conversion to the TIFF 6.0 specification.

(f) The following factors are to be considered before selecting a storage media or converting from one media to another:

1. The authorized retention of the records as determined during the scheduling process;
2. The maintenance necessary to retain the records;
3. The cost of storing and retrieving the records;
4. The access time to retrieve stored records;
5. The portability of the medium (that is, selecting a medium that can be read by equipment offered by multiple manufacturers); and
6. The ability to transfer the information from one medium to another, such as from optical disk to magnetic tape.

(11) MAINTENANCE OF ELECTRONIC RECORDS.

(a) STANDARD. Agencies shall maintain all long-term and permanent backup/security electronic recording media in a storage facility, either on-site or off-site, with constant temperature (below 68 degrees Fahrenheit) and relative humidity (20 to 30 percent) controls. Storage and handling of long-term and permanent records on magnetic tape shall conform to the standards contained in Standard AES22-1997 "AES recommended practice for audio preservation and restoration – Storage and handling – Storage of polyester-base magnetic tape," (1997) which is hereby incorporated by reference and made a part of this rule. This publication is available from the Audio Engineering Society, Incorporated, 60 East 42nd Street, Room 2520, New York, New York, 10165-2520.

(b) STANDARD. Agencies shall annually read a statistical sample of all electronic media containing long-term or permanent records to identify any loss of information and to discover and correct the cause of data loss.

(c) STANDARD. Agencies shall test all long-term or permanent electronic records at least every 10 years and verify that the media are free of permanent errors.

(d) STANDARD. Agencies shall only rewind tapes immediately before use to restore proper tension. When tapes with extreme cases of degradation are discovered, they should be rewound to avoid more permanent damage. Tapes shall be played continuously from end to end to ensure even packing. Tapes shall be stored so that the tape is all on one reel or hub.

(e) STANDARD. Agencies shall prohibit smoking, eating, and drinking in areas where electronic records are created, stored, used, or tested.

(f) STANDARD. External labels (or the equivalent automated management system) for electronic recording media used to store long-term or permanent records shall provide unique identification for each storage media, including:

1. The name of the organizational unit responsible for the data;
2. System title, including the version number of the application;
3. Special security requirements or restrictions on access, if any; and
4. Software in use at the time of creation.

(g) STANDARD. For each electronic records series, agencies shall maintain human readable information specifying the metadata associated with the series, and technical documentation specifying recording methods, formats, languages, dependencies, and schema sufficient to ensure continued access to, and intellectual control over, the series. Additionally, the following information shall be maintained for each media used to store long-term or permanent electronic records:

1. File title;
2. Dates of creation;
3. Dates of coverage; and
4. Character code/software dependency.

(h) STANDARD. Electronic records shall not be stored closer than 2 meters from sources of magnetic fields, including generators, elevators, transformers, loudspeakers, microphones, headphones, magnetic cabinet latches and magnetized tools.

(i) STANDARD. Electronic records on magnetic tape or disk shall not be stored in metal containers unless the metal is non-magnetic. Storage containers shall be resistant to impact, dust intrusion and moisture. Compact disks shall be stored in hard cases, and not in cardboard, paper or flimsy sleeves.

(j) STANDARD. Agencies shall ensure that record (master) copies of electronic records are maintained by personnel properly trained in the use and handling of the records and associated equipment.

(k) STANDARD. Agencies shall not use floppy disks, audio cassettes, or VHS-format video cassettes for the storage of record (master) copies of long-term or permanent records. Long-term and permanent records on magnetic tape shall be stored on polyester-based media. Agencies shall use only previously unrecorded videotape for original record (master) copies of long-term or permanent video recordings. For long-term or permanent audio recordings of record (master) copies, agencies shall use only one quarter inch open-reel tapes at three and three-quarters or seven and one half inches per second, full track, using professional unrecorded polyester splice-free tape stock. For long term or permanent digital recordings of record (master) copies, agencies may use open reel one-half inch tape reels recorded at 1600 or more bits-per-inch; 3480, 3490, or 3590-type tape cartridges; or compact disk read-only-memory (CD-ROM) media.

(l) Agencies shall establish and adopt procedures for external labeling of the contents of diskettes, disks, tapes, or optical disks so that all authorized users can identify and retrieve the stored information.

(m) Agencies shall convert storage media to provide compatibility with the agency's current hardware and software to ensure that information is not lost due to changing technology or deterioration of storage media. Before conversion of information to different media, agencies must determine that authorized disposition of the electronic records can be implemented after conversion. Long-term or permanent electronic records stored on magnetic tape shall be transferred to new media as needed to prevent loss of information due to changing technology or deterioration of storage media.

(n) Agencies shall back up electronic records on a regular basis to safeguard against the loss of information due to equipment malfunctions or human error. Duplicate copies of long-term or permanent records shall be maintained in storage areas located in buildings separate from the location of the records that have been copied.

(12) RETENTION OF ELECTRONIC RECORDS. Agencies shall establish policies and procedures to ensure that electronic records and their documentation are retained as long as needed. These retention procedures shall include provisions for:

(a) STANDARD. Scheduling the retention and disposition of all electronic records, as well as related access documentation and indexes, in accordance with the provisions of Chapter 1B-24, F.A.C.

(b) STANDARD. Transferring a copy of the electronic records and any related documentation and indexes to the Florida State Archives at the time specified in the records retention schedule, if applicable. Transfer may take place at an earlier date if convenient for both the agency and the Archives.

(c) STANDARD. Establishing procedures for regular recopying, reformatting, and other necessary maintenance to ensure the retention and usability of the electronic records throughout their authorized life cycle.

(13) DESTRUCTION OF ELECTRONIC RECORDS. Electronic records may be destroyed only in accordance with the provision of Chapter 1B-24, F.A.C. At a minimum each agency should ensure that:

(a) Electronic records scheduled for destruction must be disposed of in a manner that ensures protection of any sensitive, proprietary, or security information, and;

(b) Recording media previously used for electronic records containing sensitive, proprietary, or security information are not reused if the previously recorded information can be compromised in any way by reuse.

Specific Authority 257.14, 257.36(7) FS. Law Implemented 257.36(1)(a) FS. History--New 8-16-92, Amended 5-13-03.