1B-26.003 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 system 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 this rule is Sections 257.14 and 257.36(1) and (6), 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 electronic record (master) copies, regardless of the media.

3. Electronic records include numeric, graphic, audio, 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.

(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) “ASCII” means the American Standard Code for Information Interchange, a 7-bit coded character set for information interchange which was formerly ANSI (American National Standards Institute) Standard X3.4 and has since been incorporated into the Unicode standard as the first 128 Unicode characters.

(b) “Database” means an organized collection of automated information.

(c) “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.

(d) “Digital signature” means a type of electronic signature (any letters, characters, or symbols executed with an intent to authenticate) that can be used to authenticate the identity of the sender of a message or the signer of a document and to ensure that the original content of the message or document that has been sent is unchanged. Digital signatures can be created through hashing algorithms.

(e) “Electronic record” means any information that is recorded in machine readable form.

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

(g)“Hashing algorithm” (hash function, checksum) means a formula or procedure for checking that electronically transmitted messages or documents have not been altered by transforming a string of characters into a usually shorter fixed-length “hash value” or key that represents the original string. The receiver of the message can execute the same hashing algorithm as the sender and compare the resulting hash values; any difference in the hash values indicates an alteration of the message or document sent. Hashing algorithms can be used to create digital signatures.

(h) “System design” means the design of the nature and content of input, files, procedures, and output and their interrelationships.

(i) “Permanent or long-term records” means any public records as defined by Section 119.011(11), F.S. which have an established retention period of more than 10 years.

(j) “Record (master) copy” means public records specifically designated by the custodian as the official record.

(k) “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.

(l) “Open format” means a data format that is defined in complete detail, allows transformation of the data to other formats without loss of information, and is open and available to the public free of legal restrictions on use. An open format may be either standards-based or proprietary.

(m) “Unicode” means the universal character encoding standard maintained by the Unicode Consortium,

providing the basis for processing, storage, and interchange of text data in any language in all modern software and information technology protocols.

(6) AGENCY DUTIES AND RESPONSIBILITIES. 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 an individual agency-specific records retention schedule in accordance with Rule 1B-24.003, F.A.C., Records Retention Scheduling and Dispositioning.

(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 agency electronic recordkeeping systems meet state requirements for public access to records in accordance with Chapter 119, F. S.

1. STANDARD. Each agency which maintains public records in an electronic recordkeeping system shall provide, to any person making a public records request pursuant to Chapter 119, F.S., a copy of any data in such records which is not exempt from disclosure by statute. 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 Section~~s~~ 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 for electronic recordkeeping hardware, software, systems, or services if such contract or obligation impairs the right of the public under state law to inspect or copy the agency's nonexempt public records, or impairs the agency's ability to retain the records in accordance with established records retention schedules.

3. STANDARD. In providing access to electronic records, agencies shall ensure that procedures and controls are in place to maintain confidentiality for information which is exempt from public disclosure.

(7) DOCUMENTATION STANDARDS.

(a) STANDARD. Agencies 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. Documentation for electronic records systems shall be maintained in electronic or printed form as necessary to ensure access to 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, 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. 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 180-2 (FIPS-PUB 180-2) (August 1, 2002) entitled "Secure Hash Standard" (or "Secure Hash Signature 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://csrc.nist.gov/publications/fips/fips180-2/fips180-2.pdf. Agencies utilizing hashing algorithms shall only use validated implementations of hashing algorithms.

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 or Unicode format as prescribed by the Unicode 5.0 Standard (or successor Unicode Standard), which is hereby incorporated by reference, and made a part of this rule. This publication is available from the Unicode Consortium, P.O. Box 391476, Mountain View, CA 94039-1476, and at the Internet Uniform Resource Locator: http://www.unicode.org/book/bookform.html; 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 are protected 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) STANDARD. Agencies shall not use floppy disks, audio cassettes, or VHS-format video cassettes for the storage of record (master) copies of permanent or long-term records. Permanent or long-term records on magnetic tape shall be stored on polyester-based media. Agencies shall use only previously unrecorded audio or video tape for record (master) copies of permanent or long-term audio or video recordings.

(d) STANDARD. A scanning density with a minimum of 300 dots per inch is required for scanned images created by the agency from hard copy permanent or long-term records.

(e) STANDARD. Record (master) copies of scanned images created by the agency from hard copy permanent or long-term records must be stored in accordance with a published International Organization for Standardization (ISO) open standard image format.

(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 back up electronic records on a regular basis to safeguard against the loss of information due to equipment malfunctions, human error, or other disaster. Agencies shall maintain backup electronic recording media created for disaster recovery purposes, and all preservation duplicates of permanent or long-term records, in an off-site storage facility with constant temperature (below 68 degrees Fahrenheit) and relative humidity (20 to 30 percent) controls. Storage and handling of permanent or long-term records on magnetic tape shall conform to the standards contained in Standard AES22-1997 (r2003), "AES recommended practice for audio preservation and restoration – Storage and handling – Storage of polyester-base magnetic tape" (published 1997, reaffirmed 2003), 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, and at the Internet Uniform Resource Locator: http://www.aes.org/publications/standards/search.cfm. If an agency cannot practicably maintain backups and preservation duplicates as required in this section, the agency shall document the reasons why it cannot do so. Other electronic records media should be stored in a cool, dry, dark environment when possible (maximum temperature 73 degrees Fahrenheit, relative humidity 20-50 percent),

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

(c) STANDARD. Agencies shall test all permanent or long-term electronic records at least every 10 years and verify that the media are free of permanent errors. More frequent testing (e.g. at least every 5 years) is highly recommended.

(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 and copied to new media as soon as possible. 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 permanent or long-term 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 all media used to store permanent or long-term electronic records, agencies shall maintain human readable information specifying recording methods, formats, languages, dependencies, and schema sufficient to ensure continued access to, and intellectual control over, the records. Additionally, the following information shall be maintained for each media used to store permanent or long-term 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 (about 6 feet, 7 inches) 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) 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.

(l) 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. Permanent or long-term 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.

(12) RETENTION OF ELECTRONIC RECORDS. Each agency is responsible for ensuring the continued accessibility and readability of public records throughout their entire life cycle regardless of the format or media in which the records are maintained.

Agencies shall establish policies and procedures to ensure that electronic records and their documentation are retained and accessible as long as needed. These 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. 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.

(c) 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.

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

(a) Electronic records scheduled for destruction are disposed of in a manner that ensures that any information that is confidential or exempt from disclosure, including proprietary~~,~~ or security information, cannot practicably be read or reconstructed, and;

(b) Recording media previously used for electronic records containing information that is confidential or exempt from disclosure, including 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(1), 257.36(6) FS. Law Implemented 257.36(1)(a) FS. History–New 8-16-92, Amended 5-13-03, 5-21-08.