1B-26.003 Electronic Recordkeeping.

(1) These rules provide standards for record copies of public records which reside in electronic form. These **requirements must be** incorporated in the system design and implementation of new systems and enhancements to existing systems in which electronic records reside. **Public records are those as defined by Section 119.011(12), F.S.**

(2) These rules **are applicable to all agencies** as defined by Section 119.011(2), F.S., and establish minimum requirements for the creation, utilization, maintenance, retention, preservation, storage and disposition of electronic record copies, regardless of the media.

(3) Electronic recordkeeping systems and practices 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 or practices are replaced or upgraded. New and upgraded electronic recordkeeping systems and practices created or implemented after the effective date of this rule **shall comply with the requirements contained herein.** If an agency cannot practicably achieve compliance with this section in relation to an upgraded system, the agency shall document the reason why it cannot do so.

(4) For the purpose of these rules:

(a) "Checksum" means a hashing algorithm **or procedure for checking that electronic records 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.

(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 checksums.

(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) "Logical access controls" means those administrative controls and permissions allowing or limiting user access to a system's records and resources.

(h) "Metadata" means structured or semi-structured data about records that enables identification, access, use, understanding and preservation of those records over time.

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

(j) "Permanent or long-term records" means any public records as defined by Section 119.011(12), F.S., which have an established retention period of more than 10 years.

(k) "PPI" means pixels per inch and is the measurement of digital pixels on a screen or file.

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

(m) "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.

(n) "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.

(o) "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.

(5) 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:

(a) 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

(b) The physical and technical characteristics of the records, including:

1. 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

2. A data dictionary or the equivalent information associated with a database management system including a description of the relationship between data elements in databases;

(c) 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,

(d) Any other technical information needed to read or process the records.

(6) Electronic recordkeeping systems that maintain record 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. **Checksums and digital signatures should be considered for all official file copies of electronic records.** The use of automated integrity controls, such as checksums and digital signatures, can reduce the need for other security controls. Checksums used to protect the integrity of official file copies of records should meet the requirements of U.S. Federal Information Processing Standards Publication 180-4 (FIPS-PUB 180-4) (August 4, 2015) entitled "Secure Hash Standard (SHS)," https://www.flrules.org/Gateway/reference.asp?No=Ref-13888 which is hereby incorporated by reference, and made a part of this rule. This publication is available from the National Institute of Standards and Technology, U.S. Department of Commerce, 100 Bureau Drive, Gaithersburg, MD 20899, and at the Internet Uniform Resource Locator: https://csrc.nist.gov/publications/detail/fips/180-4/final.

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.

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

(b) Before a record 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.

(c) Systems or programs used to create, store or access record copies of electronic records must capture structural, descriptive, administrative and technical metadata standard to the system or program employed and must generate additional metadata whenever a record is moved within the system or migrated to another format or storage medium.

(7) 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) Professional engineer drawings and documents: Maintain in unaltered form a record copy of any and all documents signed, dated and sealed by a professional engineer prior to or upon submission to the agency. The record copy of signed, dated and sealed documents must be retained in unaltered form for the duration of the record's retention period. This provision does not prohibit agencies from scanning the unaltered document and maintaining the scanned copy as the record copy.

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

(8) For storing record 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) Agencies shall not use the following for the storage of record copies of permanent or long-term records:

1. Flash memory media (such as thumb drives, SD cards, CF cards, micro-SD cards);
2. Audio cassette tape;
3. VHS video cassette tape;
4. Floppy disks.

(d) Permanent or long-term records may be stored using one or more of the following methods:

1. Hard drive, preferably high-reliability, solid-state drive (SSD); spinning hard disk drive (HDD) is also acceptable;
2. Optical disc, preferably write-once discs with an inert dye layer;
3. Polyester-based magnetic data tape;
4. Cloud storage, preferably high-reliability, web-based storage services.

(e) Standard. A scanning density with a minimum of 300 PPI is required for scanned images created by the agency from hard copy permanent or long-term records.

(f) Record 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.

(g) 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.

(9)(a) 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. Additional backups are strongly recommended for permanent and long-term records. Backups created for disaster recovery purposes, and all preservation duplicates of permanent or long-term records, shall be maintained in an off-site storage facility, which may include cloud storage, geographically separated from the risks associated with the agency's location. The storage environment must be maintained at constant temperature (below 68 degrees Fahrenheit) and relative humidity (30 to 45 percent) levels. Storage and handling of permanent or long-term records on magnetic tape shall conform to the standards contained in Standard AES22-1997 (r2008) "AES recommended practice for audio preservation and restoration – Storage and handling – Storage of polyester-base magnetic tape" https://www.flrules.org/Gateway/reference.asp?No=Ref-13889 (published 1997, reaffirmed 2003 and 2008, stabilized 2012) which is hereby incorporated by reference and made a part of this rule. This publication is available from the Audio Engineering Society, Incorporated at the Internet Uniform Resource Locator: https://www.aes.org/publications/standards/search.cfm?docID=25. 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) 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) Agencies shall conduct data integrity testing on all media containing 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. If a checksum was previously run on the digital media, testing can be conducted by running the same checksum.

(d) Agencies shall rewind tape reels immediately before use to restore proper tension, or at a minimum every three years. 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. The requirement for rewinding does not apply to tape cartridges.

(e) 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.

(f) 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.

(g) Electronic records storage media shall not be stored closer than 6 feet to sources of magnetic fields, including generators, elevators, transformers, loudspeakers, microphones, headphones, magnetic cabinet latches and magnetized tools.

(h) 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.

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

(j) Agencies shall establish and adopt procedures for external labeling of physical storage media and for descriptive file naming and/or labeling of electronic files and directories so that all authorized users can identify and retrieve the stored information.

(k) 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 shall be transferred to new media compliant with this rule as needed to prevent loss of information due to changing technology or deterioration of storage media.

(10) Each agency is responsible for ensuring the continued accessibility and readability of public records throughout the 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) 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) 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) 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.

(11) Electronic records may be destroyed only in accordance with the provisions of Chapter 1B-24, F.A.C.

Rulemaking 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, 12-6-21.