100-RICR-50-00-2

TITLE 100 – DEPARTMENT OF STATE

CHAPTER 50 – STATE ARCHIVES, LIBRARY AND PUBLIC INFORMATION

SUBCHAPTER 00 – PUBLIC RECORDS ADMINISTRATION

PART 2 – ELECTRONIC RECORDS MANAGEMENT

2.1 Purpose

A. To ensure electronic records are retained in a trustworthy, accessible, and appropriate manner.

2.2 Authority

A. This Regulation is promulgated pursuant to the authority granted in R.I. Gen. Laws Title 38 ("Public Records"), including expressly but without limitation R.I. Gen. Laws § 38-3-1 et seq., as hereafter revised and amended (the "Public Records Administration Act").

2.3 Incorporated Material

A. These Regulations hereby adopt and incorporate by reference the following standards, not including subsequent editions or amendments thereof and only to the extent that the provisions therein are not inconsistent with these Regulations:

1. Electronic Records Management, 36 C.F.R. Part 1236 (8/28/2023);

2. National Archives and Records Administration Universal Electronic Records Management (ERM) Requirements, 2023; and

3. National Archives and Records Administration Criteria for Successfully Managing Permanent Electronic Records, 2018.

2.4 Definitions

A. For the purpose of this Part:

1. "Administrative metadata" means elements of information used to manage records and relate them to one another. Administrative metadata elements describe how a record was created, any access and use restrictions that apply to it, information about the record series (as defined in § 1.4(A) of this Subchapter) to which it belongs, and the records retention schedule (as defined in § 1.4(A) of this Subchapter) that identifies its legal minimum required retention period.

2. “Checksum”, "Digest", "Hash", "Hash code", or "Hash value" means a value that is computed on data and is used to authenticate information by indicating when a file has been corrupted or modified.

3. “Descriptive metadata” means elements of information that describe the records or set of records itself. They apply to both the source records and any versions produced through digitization. Descriptive metadata for individual source records include such elements as the title of a record, a description of its contents, its creator, and the date it was created. These elements support searching for and discovering records.

4. “Digitizing” means the process of converting paper or analog records into electronic records.

5. “Electronic information system” means an information system that contains and provides access to computerized public records and other information.

6. “Electronic mail system” means a computer application used to create, receive, and transmit messages and other documents. Excluded from this definition are:

    a. File transfer utilities (software that transmits files between users but does not retain any transmission data);

    b. Data systems used to collect and process data that have been organized into data files or databases on either personal computers or mainframe computers; and

    c. Word processing documents not transmitted on an e-mail system.

7. “Embedded metadata” means the textual components that exist alongside the content (usually binary data) within the file. Embedded metadata may be used to make self-describing digital files that contain administrative rights and technical metadata can be appropriately managed outside of a recordkeeping system.

8. “Intellectual control” means the information necessary to identify and understand the content and context of the records.

9. “Media” means the physical forms on which records are stored, such as paper, photographs, compact discs, DVDs, analog tapes, flash drives, local hard drives, or servers.

10. “Metadata” means the preserved contextual information describing the history, tracking, and/or management of an electronic document.

11. "Migration" means the process of moving data from one information system or storage medium to another to ensure continued access to the information as the system or medium becomes obsolete or degrades over time.

12. “Mixed-media files” means records in different forms of media.

    a. A file, when used in the phrase “mixed-media file,” is a group of records, regardless of location and type of media, that belong together or relate to a topic.

        (1) For example, a mixed-media case file could be a box with paper notes, audio recordings of interviews, and a CD of photographs, along with physical evidence stored separately in an evidence locker.

    b. Records in a file may be in more than one media type because of how agencies create, maintain, and use records, shifts in technology, and the topic or activity involved.

13. “Physical characteristics” means the method that information is recorded, the physical condition of the material, and the smallest level of detail present.

    a. The physical characteristics of records printed on paper include:

        (1) The type of paper (office paper, Thermofax, photographic print);

        (2) The type of printing (laser printed, fax printed, typewritten, half-toned, handwritten);

        (3) Appearance (color, inks, continuous tone or monochrome images);

        (4) Size; and

        (5) Other methods of conveying information (embossed seals, stamps).

    b. These traits determine the methods and equipment used to digitize records.

14. “Physical control” means having the information necessary to physically manage records. This includes knowing:

    a. Where the records are housed;

b. Whether any records are missing or stored separately; and

c. The records' physical form (media types, the records' dimensions, and the physical characteristics).

15. “Project plan” means a document that identifies:

a. The records that are to be digitized;

b. An estimate of their volume and of the media types that are present;

c. The image quality parameters selected to capture necessary information;

d. The date range of the records;

e. A copy of the applicable agency records schedule(s);

f. Any indexes used to maintain intellectual and physical control; and

g. A quality management (QM) section that describes:

(1) Quality assurance (QA) objectives;

(2) Quality control (QC) procedures to identify and correct errors during digitization; and

(3) The QC reports that will be used to identify and remediate errors when detected.

16. “Quality assurance" or "QA” means the proactive QM activities focused on preventing defects by ensuring that a particular product or service achieves certain requirements or specifications. A QA program is heavily dependent on QC data to search for patterns and trends. QA activities also include controlled experiments, design reviews of digitization workflows, and system tests. QA programs can improve quality by creating plans and policies or by creating and conducting training.

17. “Quality control" or "QC” means the QM activities that examine products through inspection or testing to determine if they meet predetermined specifications. The purpose is to detect defects (deviations from predetermined requirements) in products or processes.

18. “Quality management" or "QM” means the overall management functions and underlying activities that determine quality policies, objectives, and responsibilities, and that implement them through planning, control, assurance, and improvement methods within the quality system.

19. “Technical metadata” means the elements of information that describe the properties of computer files, the hardware used to create them, and the parameters used by systems to render them. Technical metadata may include elements such as a file's byte size, file format and version, color encoding, and the type of equipment used to make the file (for example, camera name or scanner manufacturer).

20. “Validating” means the process of ensuring that the records meet the requirements of this Part.

2.5 General Requirements

A. Electronic records must remain accessible for the duration of the retention period specified in their records retention schedule. "Accessible" means all electronic records must be:

1. Readable:

   a. By current, commonly available hardware and software; or

   b. Converted by the originating agency for use by another software or hardware system if the existing software or hardware is no longer current or commonly available.

2. Stored appropriately:

   a. In an electronic system accompanied by documentation of release notes, functionality, and backup provisions; or

   b. On physical storage media that is descriptively labeled and readable by commonly available hardware and software.

3. Discoverable:

   a. Within a reasonable timeframe and without excessive effort via original metadata and any metadata that is necessary to understand the content and structure of the record.

4. Properly maintained by the originating agency, which includes:

   a. Migrating when the current storage medium and/or records management system nears the end of its practical lifespan; and

   b. Avoiding proprietary storage systems, records management systems, or file formats when possible.

2.6 Selection of Electronic Records Storage Media

A. Agencies shall select appropriate electronic records storage media and systems for storing public records throughout their life cycle, which meet the following requirements:

1. Permit easy and accurate retrieval in a timely manner;

2. Retain the records in a usable format until their authorized disposition date is identified in an approved records retention schedule; and

3. Meet requirements for transferring historical records to the Rhode Island State Archives, when appropriate (§ 1.8.3 of this Subchapter).

B. Agencies shall consider the following factors before selecting a storage medium or converting from one medium to another:

1. Authorized retention of the records as determined on the records retention schedule(s);

2. Maintenance necessary to retain the records;

3. Cost of storing and retrieving the records;

4. Access time to retrieve stored records;

5. Accessibility of records over time due to software and hardware requirements;

6. Portability of the medium (selecting a medium that will run on equipment offered by multiple manufacturers); and

7. Ability to transfer the information from one medium to another.

C. Agencies shall not use removable data storage devices for the exclusive storage of long-term or permanent records.

D. Agencies shall ensure that all authorized users can identify and retrieve information stored on media external to the computer system by establishing and adopting procedures for labeling the contents of the storage devices. Identification should include:

1. The name of the organizational unit responsible for the data;

2. Descriptive title of the contents, identification of software and hardware in use at the time of creation; and

3. Security requirements or restrictions, if applicable.

E. Agencies shall ensure that information is not lost due to changing technology or deterioration of storage media by converting storage media to provide compatibility with the agency's current hardware and software.

1. Before conversion of information to a different media, agencies shall determine that authorized disposition of the electronic records can be implemented after conversion.

F. Agencies shall back up electronic records on a regular basis to safeguard against the loss of information due to equipment malfunctions or human error.

1. Duplicate copies and appropriate indexes 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.

G. Agencies shall scan documents at a density of 300 dots per inch or higher.

2.6.1 Environmental Controls

A. Agencies shall:

1. Keep food and drink away from storage media and equipment;

2. Store disks and tapes:

a. In a vertical position in a dust-free environment; and

b. At a constant temperature between 60 and 68 degrees Fahrenheit and a constant relative humidity from 35% - 45%. Frequent or extreme fluctuations in temperature and humidity can accelerate the deterioration of disks and tapes.

2.6.2 Media Controls

A. Agencies shall:

1. Avoid using removable data storage devices (CDs, thumb drives, flash drives) for the exclusive storage of long-term or permanent records;

2. Back up electronic records on a regular basis to protect against loss of information due to equipment malfunctions or human error;

3. Maintain duplicate copies in environmentally-controlled storage areas separate from their original location;

4. Annually test a statistical sample of magnetic computer tapes and disks to identify any loss of data and to discover and correct the causes of data loss;

5. Copy all long-term or permanent electronic records before the media are 10 years old to tested and verified new media, verifying that the media is free of permanent errors;

6. Keep disks and tape drives clean;

7. Keep disks and tapes away from strong electrical or magnetic fields, including telephones; and

8. Not allow unauthorized persons access to computers, tapes, disks, and documents.

2.7 Electronic Records Storage Management Systems

2.7.1 Agency Requirements

A. Agencies shall retain responsibility for managing their electronic records, regardless of whether they reside in a public, private, or community cloud, a contracted environment, or under the agency's physical control.

1. Agencies shall be responsible for monitoring changes to third-party terms of service that may affect the management of records.

2. Agencies shall be responsible for identifying what kind of social media output constitutes a public record and capturing those records appropriately.

2.7.2 System Requirements

A. All systems and networks responsible for the creation, management, and/or preservation of public records are required to:

1. Capture, manage, and preserve electronic records with appropriate metadata and must be able to access and retrieve electronic records, including electronic messages, for the full retention period listed in the associated records retention schedule (as defined in § 1.4(A) of this Subchapter) for that record;

2. Have controls for file integrity monitoring to prevent unauthorized use, alteration, concealment, or deletion of records. Examples of controls include checksums, audit trails, access lists, monitoring, and agent validation. Monitoring documentation include audit reports and the results of integrity checks;

3. Have all events and actions related to the record by person, entities, and non-person entities documented on an on-going basis once a record has been captured into a records system;

4. Document and track into an audit log any actions changing the level of access, altering the record, or changing the location of the record;

5. Ensure usability of records by:

    a. Determining if the retention period for any records is longer than the life of the system where they are currently stored;

    b. Converting records to usable formats and maintaining the link between the records and their metadata through the conversion process;

    c. Planning for the migration of records to a new system before the current system is retired;

    d. Ensuring that migration of records addresses non-active electronic records stored off-line; and

    e. Carrying out system upgrades of hardware and software while maintaining the functionality and integrity of the electronic records created in them.

B. If a third-party provider discontinues services, agencies shall continue to meet their records management responsibilities by migrating the records to another system or repository.

1. The system receiving the migrated records shall have appropriate security and records management controls in place to manage the records throughout the entire lifecycle, including preventing the unauthorized access or disposal of records.

2. During records migration, all records and associated metadata in the originating system shall be retained until the migration is complete and the destination system has been deemed reliable and secure.

2.7.3 Metadata Requirements

A. Agencies shall capture, manage, and preserve metadata associated with electronic records to ensure content, context, and structure is preserved.

1. Record metadata shall consist of information recording:

    a. The description of the content of the record;

    b. The structure of the record (form, format, and relationships between record components);

    c. The business context in which the record was created;

d. Relationships with other records and metadata;

e. Identifiers and other information needed to retrieve the record; and

f. The business actions and events involving the record throughout its existence.

B. Records systems shall define metadata to:

1. Enable the identification and retrieval of records;

2. Track processes carried out on records; and

3. Associate records with:

a. Changing business rules, policies, and mandates;

b. Agents, and their authorizations and rights with regards to the records; and

c. Their business activities.

C. Metadata shall be in one of six categories:

1. Identity - information identifying the record;

2. Description - information determining the nature of the record;

3. Use - information facilitating immediate and longer-term record use;

4. Event plan - information used to manage the record, such as disposition information;

5. Event history - information recording past events on the record and its metadata; or

6. Relation - information describing the relationship between the record and other records.

D. Metadata for a record shall be protected from unauthorized deletion and shall be retained or destroyed in accordance with the record's retention schedule.

E. Once the record has been captured, the associated metadata, including a unique identifier, author, date of creation, and relationships with other records, shall be fixed and kept as transactional evidence.

F. When migrating records between systems or converting to new file formats, agencies shall ensure informational content remains unaltered and that sufficient

metadata describing the context and structure of the records is retained to be used for all of the same business purposes as the source records.

2.8 Disposition of Electronic Records

A. Electronic records may be destroyed only in accordance with approved records retention schedules and a counter-signed Certification of Records Destruction (§ 1.8.1 of this Subchapter). Each agency shall ensure that:

1. Electronic records scheduled for destruction are disposed of in a manner that ensures protection of any confidential information;

2. Magnetic recording media previously used for electronic records containing confidential information are not reused if the previously recorded information can be compromised by reuse in any way; and

3. All back-up copies of records scheduled for disposition are also destroyed.

2.9 Severability

A. If any provision of these Regulations or the application thereof to any Person or circumstances is held invalid by a court of competent jurisdiction, the validity of the remainder of the Regulations shall not be affected thereby.

100-RICR-51-00-54

TITLE 100 - DEPARTMENT OF STATE

CHAPTER 51 - PUBLIC RECORDS ADMINISTRATION

SUBCHAPTER 00 - N/A

PART 54 - OPERATING SYSTEM TEST

Type of Filing: Adoption

Agency Signature

E-SIGNED by Rachel Strashnick on 2025-10-23 17:48:43 GMT

October 23, 2025

Agency Head Signature | Agency Signing Date

Department of State

10/24/2025

Regulation Effective Date

E-SIGNED by Department of State on 2025-10-23 17:52:16 GMT

October 23, 2025

Department of State Initials | Department of State Date