Resolution No. 10344 - Exhibit “A”

RECORDS AND INFORMATION MANAGEMENT (RIM) PROGRAM

The City relies heavily on its records to conduct business. Records support the immediate needs of municipal government and insure its continuity. Maintained over time, municipal government records preserve the history of the City of Great Falls.

Pursuant to Mont. Code Ann. §§ 2-6-1012 and 7-5-4124, the City Commission adopts this RIM Program this 5th day of May, 2020:

1.0 PURPOSE

The purpose of this Records and Information Management (RIM) Program (hereinafter “Program”) is to establish the duties and responsibilities of City personnel with respect to City records and to provide for a comprehensive system of integrated procedures for the efficient and effective management of City records, consistent with the requirements of Montana Code Annotated (MCA) Title 2, Chapter 6.

2.0 POLICY

It is hereby declared to be the policy of the City of Great Falls to provide for efficient, economical, and effective controls over the creation, distribution, organization, maintenance, use, and disposition of all City records through a comprehensive system of integrated procedures for the management of records from their creation to their ultimate disposition.

3.0 DEFINITION OF CITY/MUNICIPAL RECORDS

3.1 Public Information (§ 2-6-1002 (11), MCA)

“Public information" means information prepared, owned, used, or retained by any public agency relating to the transaction of official business, regardless of form, except for confidential information that must be protected against public disclosure under applicable law.

3.2 Public Record (§ 2-6-1002(13), MCA)

“Public record" means public information that is: (a) fixed in any medium and is retrievable in usable form for future reference; and (b) designated for retention by the state records committee, judicial branch, legislative branch, or local government records committee.

4.0 POSSESSION AND PRESERVATION OF RECORDS

All records generated and received by the City are and remain property of the City. No City official or employee has, by virtue of his/her position, any personal or property right to such records even though he/she may have developed or compiled them. City records must be delivered by outgoing City staff to their successors and must be managed, transferred, destroyed, or disposed of in accordance with state law and this Program.

- This provision applies to all records, regardless of media type, that are created, received, or maintained by the City.
- This provision includes, but is not limited to, records created on home or non-City computer equipment for work-related purposes.

5.0 RESPONSIBILITIES

The Deputy City Manager shall oversee the Program and delegates program responsibility for records and information management as follows:

5.1 Records Manager: The City Clerk is designated as the City’s Records Manager to administer the RIM Program. The Records Manager shall be responsible for:

- Monitoring Local Government Records Committee Records Retention Schedules; the provisions of Mont. Code Ann. Title 2, Chapter 6; and Administrative Rules issued by the State of Montana
- Serving as the primary contact for Records Custodians and Records Coordinators pertaining to records retention
- Training and keeping designated Records Coordinators updated on changes to laws, rules, or retention schedules
- Creating and updating as necessary a “Request for Authorization for Records Disposal or Destruction” form (hereinafter “records disposal form”) for use by all City departments
- Processing all City department records disposal forms. The City Clerk’s Office shall be the office of record for completed records disposal forms to maintain the identity of City records approved for disposal, destruction, or transfer under the approved records retention schedules
- Submitting the appropriate documentation to the State for approval of disposal, destruction, or transfer of City records over 10 years old
- Submitting the appropriate documentation to the Local Government Records Committee regarding proposed amendments or additions (new records series) to retention schedules
- Reporting regularly to the Deputy City Manager on the compliance and effectiveness of the Program in each City department
- Bringing to the attention of the Deputy City Manager noncompliance by City staff with the Program.

5.2 Records Custodians

All City employees are records custodians and are responsible for the management of the Department records in their custody and care. This includes, but is not limited to:

- Proper retention of City records that are created, sent, or received; and
- Proper approval before destroying or disposing of City records.

5.3 Department Directors

All directors of City departments are responsible for the implementation and operation of effective file operations, records transfers and dispositions, and other activities in accordance with the provisions of this Program within their areas of responsibility. They shall notify the Records Manager of their department’s designated staff member to serve as a Records Coordinator. In the event of the resignation, retirement, dismissal, or removal of a person designated as a Records Coordinator, the Department Director shall promptly designate another staff member and so notify the Records Manager.

5.4 Records Coordinators

The Records Coordinator is responsible for coordination between personnel in his/her department to ensure compliance with the provisions of this Program. This responsibility shall include:

- Being thoroughly familiar with all records created and maintained by the department
- Carrying out the procedures of the Program in their department and keeping departmental staff apprised of any changes or updates to the Program or Records Retention Schedules
- Supervising the application of records retention schedules within the department and submitting records disposal forms to the Records Manager
- When necessary, advising the Records Manager of the need for amendments to Records Retention Schedules
- Reporting any violations of the Program to the Department Director and Records Manager.

5.5 Information Technology (IT) Manager

The IT Manager is responsible for:

- Maintaining electronic records on City electronic information systems
- Ensuring various degrees of protection to electronic records and information that are either private, confidential, or essential to the City’s continuity or that otherwise require protection
- Ensuring that any City records management solution is secure, that it is of the proper scale, that it is reliable, and that it communicates with the document management services and e-mail servers that supply it with records
- Routinely backing up electronic information to ensure that it can be restored if there is a disaster, a system malfunction, or data corruption
- Periodically testing and migrating electronic information, including all appropriate metadata, to current supported hardware and/or converted with current software to new versions and/or formats to sustain its on-going accessibility

- Notifying staff of technology changes that would affect access, retention, or disposition (archiving or disposing) of records in electronic information systems.
- Ensuring that contracts with vendors meet the City's ability to identify, locate, and retrieve the records and information required to support its ongoing business activities

5.6 City Attorney

The City Attorney or designee shall be responsible for confirming whether or not the subject matter of any record on the records disposal form is pertinent to a pending legal or regulatory hold or lawsuit.

6.0 APPRAISING RECORDS

6.1 Administrative Value

Most records are created as administrative tools to help accomplish the functions for which municipal government was established. In most cases, the primary administrative value of a record will be exhausted when the transaction to which it relates is completed.

6.2 Legal Value

If a record contains evidence of a legally enforceable right or obligation of government, then it probably has legal value. Among these types of records are those that show the basis for an action (legal decisions, opinions), financial and other documents representing legal agreements (leases, titles, contracts), and records of actions taken in a particular case (claims, dockets). The legal value of a record will often be evident from its title, such as a contract, purchase order, lease, title, deed, charter, some personnel records, and certain medical records.

6.3 Fiscal Value

To fulfill its financial obligations, municipal government records such as budgets, ledgers, payrolls, vouchers, warrants, and encumbrances need to be kept and maintained. These records all have fiscal value, as would almost any document needed for a fiscal audit.

6.4 Essential Record

An essential record is a public record that provides for the continuity and preservation of local government and may be immediately necessary to respond to an emergency or disaster or begin recovery or reestablishment of operations during and after an emergency or disaster. The City shall collaborate with the appropriate continuity of government programs to ensure essential records are identified, maintained, stored, and backed up.

6.5 Non-Records: Non-records are those that have no operational value, can be destroyed when no longer needed, and need no disposal approval. Examples include courtesy copies of other entities' publications/journals, spam email, blank forms, etc.

Additionally, when an office of record is designated for particular records, duplicate copies kept only for reference can be disposed of/destroyed when no longer needed, and need no disposal approval. For example, the Finance Department is the office of record for processing accounts payable records submitted by other departments. Any copies maintained by staff in other departments for reference purposes can be disposed of when no longer required. Duplicate records should not be retained longer than the “record” copy.

7.0 RECORD RETENTION

Record retention is the period of time during which records must be legally retained or are operationally required in a certain location or format.

7.1 Local Government Records Committee

The Legislature created the Local Government Records Committee (§ 2-6-1201, MCA) to oversee the preservation and disposal of public records kept by local governments. The Local Government Records Committee approves, modifies, or disapproves proposals for local government records retention and disposition schedules (§ 2-6-1202, MCA) and provides guidelines for local government’s digital records creation, preservation and data migration.

7.2 Records Retention Schedules

Retention requirements that are specifically set forth herein and Records Retention Schedule documents define the City’s legal and compliant recordkeeping requirements. The City adopts all applicable Records Retention Schedule documents approved by the Local Government Records Committee set forth at: https://sosmt.gov/Records/Local/. All City Departments shall comply with the specific retention requirements set forth herein and the Records Retention Schedules in order to ensure that department records are kept as long as legally and operationally required, and that non-records and obsolete records are disposed of in a systematic and controlled manner. Schedule 8 (Municipal Records Schedules) will be applicable to most City Department records. Complying with the retention requirements set forth herein and the Records Retention Schedules ensures that employees adhere to approved recordkeeping requirements, and that they do so consistently.

7.3 Implementation of Records Retention Schedules; Disposal, Destruction or Transfer of Records

Once records have met the minimum retention period set forth herein or according to the applicable Records Retention Schedule, the following process shall be followed:

- The Records Coordinator shall complete and sign the records disposal form and present it to his/her Department Director for review and signature
- When signed by the Records Coordinator and Department Director, the Records Coordinator shall forward the records disposal form to the Records Manager
- The Records Manager will confirm that the records meet the minimum retention requirements, determine whether an open records request is pending for any of the records, and then forward the records disposal form to the City Attorney
- The City Attorney or designee will confirm whether or not the subject matter of the record is pertinent to a pending legal or regulatory hold or lawsuit

- Once the records disposal form is signed by the Records Manager and City Attorney, the records disposal form will be routed to the Deputy City Manager for review and signature
- Once the records disposal form is fully executed, the disposal or destruction of records is approved.

The Records Manager shall communicate instructions to the submitting Records Coordinator to complete the certification portion at the bottom of the records disposal form when the records have been appropriately disposed of or destroyed and to return the fully completed records disposal form to the City Clerk's Office for official filing.

Should any of the records submitted for disposal by any City department be more than 10 years' old, the Records Manager shall submit the appropriate forms to the Secretary of State Local Government Records Committee for approval of disposal or transfer or for notification to the Central Registry pursuant to Mont. Code Ann. § 2-6-1205.

Notwithstanding minimum retention periods, all records must be maintained until all required audits are completed and should be retained beyond the listed retention periods when there is a probability of litigation involving records or a probability that their use will be required in the future.

8.0 CUSTODY OF RECORDS; REMOVAL

8.1 Office of Record: The Office of Record is the departmental office that has the official responsibility to maintain a particular record series.

8.2 Active Records: The originating department has full custody over records still in active use.

8.3 Inactive Records: The originating department is the legal custodian of its records in storage and shall retain the authority to retrieve and use records deposited in inactive storage.

8.4 Archived Records: The Public Works Engineering Division and the City Clerk's office files shall be combined and transferred to the Records Manager's archives when an office file is closed. Records may be temporarily removed from the archives at the request of City staff by requesting same from the Records Manager and completing the Archived Office File Check-Out Form. Records transferred to or acquired for the archives shall be under the full custody of the Records Manager.

9.0 PRESERVATION OF PERMANENT RECORDS

The Records Manager maintains historical and archived permanent records that are not used in the day-to-day operations of the City, as well as maintains records of Transfer Receipts of records transferred to the Cascade County Historical Society/History Museum for perpetual care and preservation, or other appropriate entity not contrary to law or regulation.

10.0 ELECTRONIC RECORDS: Information captured through electronic means which may or may not have a paper record are electronic records. Examples include electronic mail messages (e-mail); Word or Excel documents; electronically created, scanned, or stored records or databases; digital images; and social media.

Electronic records can encompass both analog and digital information formats, although the term principally connotes information stored in digital computer systems. “Electronic records” most often refers to records created in electronic format (born digital), but is sometimes used to describe scans of records in other formats (reborn digital or born analog). Electronic records are often analogous to paper records, email to letters, word processing files to reports, and other documents.

All of these types of documents must be stored on a server, such as the City’s Common Drive, to ensure proper retention, backup, maintenance, and migration by the IT Department. Should the City propose to utilize vendor(s) for such services, the contract shall first be reviewed and approved by the IT Manager and City Attorney or attorney designee.

The City shall utilize the most current version of the *Digital Records Creation and Preservation Guidelines for Local Government* issued by the Montana State Archives and Local Government Records Committee as a resource for the effective creation and preservation of electronic records.

Original electronically stored documents with less than a 10-year record retention schedule may be maintained without maintaining a copy in another medium. When such records have met the minimum required retention period, Records Coordinators shall submit a completed records disposal form to the Records Manager for processing as set forth above in Section 7.3.

The City adopts and incorporates by reference the Association of Records Managers & Administrators (ARMA) International’s *Generally Accepted Recordkeeping Principles* for local governments using electronic systems to store long-term records (more than a 10-year retention period). When such records have met the minimum required retention, Records Coordinators shall submit a completed records disposal form to the Records Manager for processing as set forth above in Section 7.3.

10.1 Electronic mail: Electronic Mail (E-mail) is a City/Municipal public record when it is created or received in the transaction of public business as defined in Section 3 above. Email itself is not considered a record series. Email is simply a medium that creates and transmits records that have retention periods. Email and attachments are subject to the same retention requirements as traditional paper.

Personal email accounts shall not be used for the conducting of government business. However, if a record is created or received in a personal email account, it shall be forwarded to the greatfallsmt.net email system or printed to paper for appropriate recordkeeping and retention within two (2) business days.

The City utilizes an archiving solution to capture and store all incoming and outgoing electronic mail and attachments. All data is captured and stored regardless of whether the user deletes the email or not. Pursuant to the Local Government General Records Schedule #1, captured e-mail will be retained and archived for a period of four (4) years after the last date a backup was run by the IT Department. When so notified by the IT Operations Manager that certain archived emails have met the required retention period, the Records Manager shall send out a City-wide email notifying employees of the intention to initiate a records disposal form for emails within a certain date range. Within thirty (30) calendar days of said notification, staff shall print, file, and appropriately retain emails and attachments with longer than four-year retention periods. After the 30-day notification period, the Records Manager shall then complete and process the records disposal form as set forth above in Section 7.3.

10.2 Social Media: The City of Great Falls' use of social media is for informational purposes only. Any content in a social media format that is related to City business, including a list of subscribers and posted communications, is considered a public record and subject to records retention schedules. Elected officials utilizing social media in an official capacity and site administrators authorized by the Department Director (hereinafter "Site Administrators") to publish content to City-connected social media sites must also comply with the City of Great Falls Social Media Guidelines and Usage Policy. In the event of the resignation, retirement, dismissal, or removal of a person designated as a Site Administrator, the Department Director shall promptly designate another staff member and so notify the IT Manager and Communication Specialist.

The City utilizes an archiving solution to capture, archive, and maintain records of City-connected social media account activity to comply with applicable public records laws and to fulfill record retention requirements. Social media Site Administrators are responsible for coordinating with the Records Manager to respond completely and accurately to any public records request for social media content.

Social media posted communication is transitory in nature. Captured social media content that does not violate the archiving solution's policies, shall be retained for a minimum period of one (1) year. After archived social media content has met the one-year retention period, the Records Manager shall send out an email notifying Site Administrators of the intention to initiate a records disposal form for social media content within a certain date range. Site Administrators shall notify the Records Manager within thirty (30) calendar days of said email notification if it is determined that certain content may need to be retained for a longer period of time. After the 30-day notification period, the Records Manager shall then complete and process the records disposal form as set forth above in section 7.3.

10.3 Records Retained on Digital Media

Audio recordings of City Board, Commission, and Council meetings shall be retained for a period of one year after written minutes are completed and approved or the proceedings are completely transcribed, whichever is appropriate. The Records Coordinator shall complete and submit the records disposal form to the Records Manager for processing as set forth above in section 7.3.

Video recordings made by the City Clerk/City-190 Coordinator or designee of City Board, Commission, and Council meetings shall be retained for a period of three (3) years. After the recordings have met the three-year retention period, the Records Manager shall initiate a records disposal form as set forth above in section 7.3 for processing.

The City utilizes security technology at certain locations. Security video generated by security cameras/systems owned by the City shall be set to retain DVR-recorded content for a minimum of thirty (30) days unless the video becomes part of an official investigation or case file and then shall be retained as long as the relevant record series. If a Department Director determines that a longer retention period is appropriate, he/she shall make arrangements with the security company to reset the DVR content retention, and shall notify the Records Manager and Risk Management Specialist of the determined retention period.

No Disposal Form shall be initiated for DVRs set to write over video content after meeting the minimum retention period.

11.0 RECOVERY OF CITY RECORDS: The City Attorney may take steps to recover local government records which have been removed or wrongfully retained from proper custody and may, when necessary, institute actions of records recovery or replevin on behalf of the City.

Attachments: Digital Records Creation and Preservation Guidelines for Local Government
Generally Accepted Recordkeeping Principles

Digital Records Creation and Preservation

Guidelines for Local Government

Montana State Archives
and Local Government Records Committee
Draft, July 2019

Table of Contents

INTRODUCTION

This document provides guidelines to local government entities regarding the effective creation and preservation of digital files, whether born-digital records or digitized copies of records in an analog format (e.g., paper or photos). It provides considerations for digitization, file formats, file naming, storage, and preservation, all important considerations when building an effective electronic records program.

An electronic records program will have four goals:

Accurate and trustworthy records

> Trustworthy electronic records contain information that is reliable and authentic. A key aspect to trustworthiness is legal admissibility, acceptance by auditors and meet legal and regulatory compliance obligations.

Complete records

> Electronic records should be complete and unaltered through tampering or data corruption. They should have all the information necessary to ensure their long-term usefulness including their content, context and structure. Content is the substance of the record. Context is often metadata like author, date last edited/printed/saved, message headers, routing/approval, Structure is the appearance and

arrangement of the content including fonts, formatting, page breaks, e-mail attachments, colors.

Accessible

Electronic records must remain available, accessible and the information they contain must be readable for their lifecycle. Electronic records require a tool like an index or strict file naming conventions to ensure they are findable.

Durable

Electronic records must be stored in an appropriate manner so they are accessible for the designated retention period. File formats, software, hardware, storage media are all subject to obsolescence. Electronic records and the systems necessary to render them must be secure from hacking, data corruption, and accidental modification or deletion. Business continuity plans must include strategies to recover electronic records.

PRESERVATION STRATEGIES

Deciding how to create, name, and store digital files affects the ability to preserve them for long-term access and use. Addressing the issues stated below will greatly increase your organizations capacity to manage, access, and preserve digital files.

- Balancing image quality and storage capacity when digitizing records to increase access to information at an affordable price.
- Electing nonproprietary file types when possible to reduce the risk of software obsolescence over time.
- Employing a consistent file naming system and metadata schema to help you find records quickly.
- Using modern storage media with a robust backup plan in place and developing a preservation strategy to help protect and maintain your files for their entire lifecycle.

SERVICES FOR LOCAL GOVERNMENTS

These guidelines have been written for organizations that digitize and store their own records. Additional guidance and services are provided by:

- The Montana Secretary of State Records Management Division offers services to assist Montana local government entities with digitization projects.
- The Montana State Archivist and members of the Archives Staff are available for consultation on preservation and access issues for electronic records (jofoley@mt.gov).
- Members of the Local Government Records Committee are also available for consultation.

DIGITIZATION:

Government agencies digitize records to increase access, streamline workflows, and reduce the need for physical storage space. Digital files made available over the web allow government agencies to provide information to partners or the public quickly and efficiently. In addition, when optical character recognition (OCR) software is used, digital images can be text-searchable, which makes information easier to find.

While digitization can save agencies time in accessing records and money in storage, it is an investment. In-house digitization requires scanners, scanning software, and storage media that should be updated on a routine basis. Keeping your software and equipment current is important to the long-term preservation of your records and will help ensure a trustworthy management and storage environment for as long as the records retention schedules require. Likewise, with vendors doing the digitization, ongoing issues with storage, preservation and access demand time and attention.

Agencies sometimes ask us if they can digitize (or scan) their paper records and then discard the paper copies. The short answer to that question is "it depends".

The Uniform Electronic Transactions Act (MCA 30-18-101 to 118) state "Each governmental agency shall determine whether, and the extent to which, it will create and retain electronic records and convert written records to electronic records".

The Montana Records Act provides government records creators with guidance "…to ensure efficient and effective management of public records and public information." It details the responsibilities of government entities to manage their records via retention schedules and the retention guidelines they provide.

Montana ARM 44.14.201 and 44.14.202 allow Local Governments to retain official records in digital format, and provide guidance on how those records should be stored to ensure long-term to permanent retention as required by retention schedules (see schedules here).

As long as the agency meets the requirements set forth in the Uniform Electronic Transactions Act, the Montana Records Act , and the guidelines set within the ARM (above) and by the Local Government Records Committee, a government agency may scan and dispose.

However, all records, unless the disposition on the applicable retention schedule states "No RM 60 required", must go through the disposal request process (see https://sosmt.gov/records/local). As provided in that process the State Archives may deem the records to be historically significant and may request the records be transferred to their facility.

In addition, any records over ten years old are subject to MCA 2-6-1205, which requires that such records be placed on central registry (listserv) that offers such records to the public prior to disposal. This "ten-year rule supersedes the "No RM 60 Required" designation. Contact SOS for details concerning the listserv, and the Local Government Records Committee with any questions about disposal requests.

Successful Digitization is dependent on good Image Quality:

General guidelines: See state tech guidelines at https://sosmt.gov/Portals/142/Records/forms/DocumentImagingTechStandard.pdf

Image quality for digitization is an important consideration, whether for short or permanent retention. Below are guidelines to assist in ensuring the quality of images allow for retention and access to digitized records.

Terms

Digitization: A process by which a document or photo is scanned and converted from analog format to a computer-readable digital format. After scanning, the document or photo is represented by a series of pixels arranged in a two-dimensional matrix called a bitmap or raster image. This image can then be kept on a network for storage and use.

Pixel Bit Depth: Pixel bit depth refers to the number of bits used to define each pixel. The higher the bit depth, the more tones (color or grayscale) can be represented in a digital image. Digital images can be bi-tonal, grayscale, or color. In general, higher bit depths are recommended for master images to accurately represent the original document.

Standard pixel bit depths

Bit-depth	Displays	Recommended for
1-bit or "bi-tonal"	black and white	Typewritten documents
8-bit grayscale	256 shades of gray	Black and white photographs, half-tone illustrations, handwriting
24-bit color	Approximately 16 million colors	Color graphics and text, color photographs, art, drawings, maps

Resolution: The quality of a digital image is dependent upon the initial scanning resolution. Resolution refers to the number of dots, or pixels, used to represent an image, expressed commonly as “dpi,” dots per inch. You may also see the terms “ppi” (pixels per inch) and “lpi” (lines per inch) used. As the dpi value increases, image quality increases, but so does the file size.

Recommendations

The desired image quality and the storage capacity of your computer system play large roles in determining what pixel bit depth and resolution to use. The greater the bit depth and resolution, the more storage space the scanned image will require. Larger images take longer to deliver over the Internet, something to consider if that is a service you provide. If online access is important to your agency, you may want to scan high-resolution masters for long-term preservation and lower resolution copies for web delivery.

In most cases, the State Archives recommends scanning standard black and white documents bi-tonal at 300 dpi. The size and quality of the original document may affect how we scan, but that is our usual resolution. Please see the table below for recommendations on scanning photographs and other record types.

Common Scanning Resolutions for Master Files

Material	Recommended resolution (8-bit grayscale and 24-bit color)
Textual records	300-600 dpi
Photographs, negatives, slides	4000-8000 pixels in long dimension

Standards for digital audio and video are complex and quickly changing, please contact the Montana State Archives for more information.

Guidelines for further reference:

- State technical guidelines https://sosmt.gov/Portals/142/Records/forms/DocumentImagingTechStandard.pdf
- Federal Agencies Digitization Guidelines Initiative: http://www.digitizationguidelines.gov/
- Council of State Archivists Minimum Digitization Capture Recommendations https://www.statearchivists.org/resource-center/resource- library/minimum-digitization-capture- recommendations/?ccm_paging_p=12

File Formats:

File formats used to create, and store content determine future viability and usage. Technology continually changes, and contemporary hardware/software should be expected to become obsolete over time.

Consider now how your data will be read if the software used to produce it becomes obsolete. File formats created with these considerations in mind are more likely to be accessible in the future.

- Non-proprietary
- Open, documented standards
- Unencrypted
- Uncompressed, if space is available

Examples of preferred formats (see Digitization section for conversion of analog content)

File Type	Preferred Format
Image	jpeg, jpeg-2000, tiff
Text	txt, html, xml, PDF or PDF/A Open Office XML
Audio	afif, wav
Video	mp4, avi
Databases	xml or convert to csv

Examples of proprietary formats and alternatives

Proprietary Format	Alternative Format
Excel (.xls, .xlsx)	Comma Separated Values (.csv)
Word (.doc, .docx)	PDF or PDF/A
PowerPoint (.ppt, .pptx)	PDF or PDF/A
Photoshop (.psd)	Tiff
QuickTime (.mov)	mpeg-4 (.mp4)

These are examples of commonly used proprietary formats. For long- term accessibility, consider generating a copy in one of the preferred formats listed in the previous section. For advice on generating these copies, contact your IT staff or the State Archives.

The following links provide more information on format descriptions and their characteristics:

- Library of Congress' Sustainability of Digital Formats: http://digitalpreservation.gov/formats/fdd/descriptions.shtml
- Council of State Archivists File Format Comparison Projects: https://www.statearchivists.org/resource-center/resource- library/guidelines-file-format-comparison-projects/?ccm_paging_p=9

File Naming

If you create and follow a specific strategy for how you name original files, you will be able to more easily identify, locate and share those files. Ideally, members of your organization should be able to look at a record's file name and use that information to recognize the contents and characteristics of the record and make decisions about it.

When developing your file naming policy, you may wish to include some of the following elements:

- Create unique file names. Duplicate file names will cause confusion.
- File names should be simple and easy to understand.
- Avoid using special characters such as: ? / $ % & # . \ : < >
- Use underscores (_) and dashes (-) to represent spaces.
- Use leading zeros with the numbers 0-9 to facilitate proper sorting and file management.
- Dates entered in this format will remain in chronological order: YYYY_MM_ DD or YYYYMMDD. Variations include YYYY, YYYY-MM, YYYY-YYYY.
- Keep the file name as short as possible and always include the three-character file extension (e.g., .jpg or .doc).
- Include the version number in the file name by using 'v' or 'V' and the version number at the end or beginning of the document. (e.g., 2014_Notes_v01.doc). Avoid using the words "version" or "draft"

Metadata

Metadata is used to describe a record, its relationships with other records, and how the record has been and should be treated over time. Metadata often includes items like file type, file name, creator name, and date of creation. Metadata enables proper data creation, storage, and retention. In addition, standardized metadata helps validate the trustworthiness of your recordkeeping system and the legal admissibility of your digitized records in court.

There are two commonly used approaches to storing metadata. Metadata can be stored separately from the digital files in a database or it can be embedded in a digital file. Most software applications automatically create metadata and associate it with files, generally making the standardization of metadata simpler.

One example of automatic and standardized metadata is the header and routing information that accompany an e-mail message. Another is the set of properties created with every Microsoft Word document; certain elements such as the title, author, file size, etc., are automatically created, but other elements can be customized and created manually.

By standardizing the process, it will be easier to manage, access, and preserve the files long-term. Normally, some combination of automatically and manually created information is best for precise and practical metadata.

Suggested metadata include:

- **TITLE:** The name given to the resource by the creator or publisher.
- **CREATOR:** The person(s) or organization(s) primarily responsible for the intellectual content of the resource; the author.
- **SUBJECT**: The topic of the resource; also, keywords, phrases or classification descriptors that describe the subject or content of the resource.
- **DESCRIPTION**: A textual description of the content of the resource, including abstracts in the case of document-like objects; also, may be a content description in the case of visual resources.
- **PUBLISHER:** The entity responsible for making the resource available in its present form, such as the county or office.
- **CONTRIBUTORS**: Person(s) or organization(s) in addition to those specified in the CREATOR element, who have made significant intellectual contributions to the resource but on a secondary basis.
- **DATE**: The date the resource was made available in its present form.
- **TYPE**: The resource type, such as home page, working paper, minutes or technical report.
- **FORMAT**: The data representation of the resource, such as text/html, ASCII, Postscript file, executable application or JPG image.

- **IDENTIFIER:** A string or number used to uniquely identify the resource. Examples from networked resources include URLs and URNs (when implemented).
- **LANGUAGE:** The language(s) of the intellectual content of the resource.
- **RIGHTS MANAGEMENT:** A link (URL or other suitable URI as appropriate) to a copyright notice, a rights-management statement or perhaps a server that would provide such information in a dynamic way.

Contact the State Archives for guidance.

Storage of Master Files:

Just as local governments were responsible for good storage of microfilm, they are responsible to ensure good stable storage for digital master files. It is critical to store digital master files in a manner that ensure they are secure, tamper proof and available if needed.

Data backup procedures should include guidelines for:

- Frequency
- Testing
- Media replacement
- Recovery time
- Roles and responsibilities

Frequency:

a) Primary backup: The recovery point objective (RPO) must be no earlier than the end of the previous business day.
b) Offsite backup: Institutions must maintain a monthly full backup offsite at a minimum of 7 miles (suggested 45 miles) from their primary data center.

Testing: Restoration of backup data must be performed and validated on all types of media in use at least every six months.

Media Replacement: Backup media should be replaced according to manufacturer recommendations.

Recovery Time: The recovery time objective (RTO) must be defined and support business requirements.

Roles and Responsibilities: Appropriate roles and responsibilities must be defined for data backup and restoration to ensure timeliness and accountability.

Offsite Storage: Removable backup media taken offsite must be stored in an offsite location that is insured and bonded or in a locked media rated, fire safe.

Onsite Storage: Removable backup media kept onsite must be stored in a locked container with restricted physical access.

Encryption: Non-public data stored on removable backup media must be encrypted. Non-public data must be encrypted in transit and at rest when sent to an offsite backup facility, either physically or via electronic transmission.

Third Parties: Third parties' backup handling & storage procedures must meet system, or institution policy or procedure requirements related to data protection, security and privacy. These procedures must cover contract terms that include bonding, insurance, disaster recovery planning and requirements for storage facilities with appropriate environmental controls.

PRESERVATION STRATEGIES

Preservation is accomplished for digital content – whether "born-digital" or the result of digitization – through the creation and maintenance of appropriate master files with accompanying structural, descriptive, and administrative metadata. These master files (with metadata) should then be ingested into a well-managed digital archive that employs robust security measures, persistent identifiers, verification mechanisms, replication of the files in geographically distinct locations, and continuous monitoring and management of the files.

Management of the files should include emulation, migration of files to new formats, and / or creation of new copies in new formats to render the content usable in diverse present and future electronic environments.

Once you have decided on a file format and a storage plan, the challenge will be to keep those files accessible and viable.

There are two, often compatible approaches for long-term electronic record preservation:

- Conversion. When you convert a record, you change its file format. Often, conversion takes place to make the record software available in an open or standard format. For example, you can convert a record created in Microsoft Word by saving it as a Rich Text Format (RTF) file or to PDF/A.
- Migration. When you migrate a record, you move it from one computer platform, storage medium, or physical format to another. For example, you may need to migrate records from old magnetic tapes to new ones or to a different medium entirely to ensure continued accessibility.

See Appendix A for sample preservation/migration planning document.

Appendix A: Generally Accepted Recordkeeping Principles®

The Generally Accepted Recordkeeping Principles® (Principles) constitute a generally accepted global standard that identifies the critical hallmarks and a high-level framework of good practices for information governance – defined by ARMA International as a "strategic, cross-disciplinary framework composed of standards, processes, roles, and metrics that hold organizations and individuals accountable for the proper handling of information assets. Information governance helps organizations achieve business objectives, facilitates compliance with external requirements, and minimizes risk posed by sub-standard information-handling practices. Note: Information management is an essential building block of an information governance program."

Published by ARMA International in 2009 and updated in 2017, the Principles are grounded in practical experience and based on extensive consideration and analysis of legal doctrine and information theory. They are meant to provide organizations with a standard of conduct for governing information and guidelines by which to judge that conduct.

Principle of Accountability: A senior executive (or a person of comparable authority) shall oversee the information governance program and delegate responsibility for information management to appropriate individuals.

Principle of Transparency: An organization's business processes and activities, including its information governance program, shall be documented in an open and verifiable manner, and that documentation shall be available to all personnel and appropriate, interested parties.

Principle of Integrity: An information governance program shall be constructed so the information assets generated by or managed for the organization have a reasonable guarantee of authenticity and reliability.

Principle of Protection: An information governance program shall be constructed to ensure an appropriate level of protection to information assets that are private, confidential, privileged, secret, classified, essential to business continuity, or that otherwise require protection.

Principle of Compliance: An information governance program shall be constructed to comply with applicable laws, other binding authorities, and the organization's policies.

Principle of Availability: An organization shall maintain its information assets in a manner that ensures their timely, efficient, and accurate retrieval.

Principle of Retention: An organization shall maintain its information assets for an appropriate time, considering its legal, regulatory, fiscal, operational, and historical requirements.

Principle of Disposition: An organization shall provide secure and appropriate disposition for information assets no longer required to be maintained, in compliance with applicable laws and the organization's policies.

Learn More: For a full explanation of how to use the Principles and the complementary Information Governance Maturity Model as guidance for developing an effective information governance program, see Implementing the Generally Accepted Recordkeeping Principles® (ARMA International TR 30-2017), which is available for purchase in the

ARMA bookstore. (For ARMA International professional members, it is a FREE PDF download. Not a member? Learn more about its benefits by visiting https://armainternational.site-ym.com/page/JoinARMA or by contacting our membership team at members@armaintl.org for personal assistance.)

ARMA International (www.arma.org) is a not-for-profit professional association and a global authority on governing information as a strategic asset. Formed in 1955, ARMA International's mission is to empower the community of information professionals to advance their careers, their organizations, and the profession.

Please cite as: Generally Accepted Recordkeeping Principles® ©2017 ARMA International, www.arma.org.

Appendix B: Template 1

Electronic Records Preservation and Data Migration Plan

^Local Government Name^ ^Program Name^

Introduction

This document is created in accordance with state law pertaining to public records and information, and based on guidance provided by the Local Government Records Committee to ensure ^Local Government Name^ ^Program Name^ is properly managing, preserving and providing access to public records and information in their care.

The Montana Records Act (see https://leg.mt.gov/bills/mca_toc/2_6_10.htm) seeks to ensure the "efficient and effective management of public records and public information, in accordance with Article II, sections 8 through 10, of the Montana constitution, for the state of Montana." It defines what constitutes a public record and/or information, and outlines the duties of government entities to preserve and protect the reliability, authenticity, integrity and usability of same regardless of format.

Montana ARM 44.14.201 and 44.14.202 allow Local Governments to retain official records in digital format, and provide guidance on how those records should be stored to ensure long-term to permanent retention as required by retention schedules (see schedules here).

44.14.201 USE OF ELECTRONIC RECORDS STORAGE SYSTEMS FOR LOCAL GOVERNMENT DOCUMENTS

(1) Electronic records storage systems may be used for the daily management, storage and retrieval of documents with a retention schedule of 10 years or more (long-term documents) or records with a retention schedule of less than 10 years (short- or medium-term documents).

44.14.202 STORAGE REQUIREMENT FOR ELECTRONICALLY STORED DOCUMENTS WITH GREATER THAN TEN YEAR RECORD RETENTION (LONG-TERM RECORDS)

(1) The Local Government Records Committee adopts and incorporates by reference the Association of Records Managers & Administrators (ARMA) International's Generally Accepted Recordkeeping Principles® for local governments using electronic systems to store long-term records, ©2014 ARMA International, www.arma.org. Local governments should use them as the framework to design, implement, operate, and decommission the systems and to manage the records and data within the systems. (see Appendix B for summary)

Purpose

The purpose of this document is to ensure that ^Local Government Name^ ^Program Name^ is setting forth the protection protocols and practices necessary to keep

official, digital records readable and accessible, for their entire lifecycle. This is true, whether a record is being kept for 2 years or 200 years. Protocols and practices include, but are not limited to, upgraded software migrations, data or records conversions, refreshment cycles for long-term or permanent records, etc.

Definitions

- **Digitization**: process of transforming analog material into binary electronic (digital) form, especially for storage and use in a computer.
- **Migration**: 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.
- **Non- proprietary (open) file types**: file format for storing digital data, defined by a published specification usually maintained by a standards organization, and which can be used and implemented by anyone.
- **Preservation Plan**: document showing systematic series of actions to prepare the electronic records for verification and preservation, including (but not limited to) file format standards, naming conventions,

Migration Plan Statement

Changes in technology may bring about changes in underlying business processes. Increased electronic capacity may become available. The age or characteristics of the electronic media that is in use may require migration from on media source to another. The **^Local Government Name^ ^Program Name^** commits to comply with state law and migrate electronic data and

records to new media and or new supporting software prior to obsolescence.

The Migration Plan constitutes the guidelines for the migration of electronic records and data to new media or to new software. ^Program Name^, the records and data business owner and staff pledge to:

- use open non-proprietary file formats to save records on selected media,
- use robust testing methods to prevent, detect and report errors when saving files to digital media to ensure they are not corrupt,
- select storage media that is sufficient for the records in terms of access, storage, usability and retention and commit to replacing and updating the media and any system required to read and access it before it obsolesces,
- know the lifecycle (longevity) of stated records,
- understand the selected storage media's expected duration and durability (i.e. computers are not being sold with CD drives now, or a file storage server's mean time between replacements and mean time between failure rating)
- determine a favorable cost/benefit ratio, and
- identify methods for recovering records from potential loss.

The ^Local Government Name^ ^Program Name^ commits to ensure the electronic record's content, structure and context are preserved throughout the record's entire lifecycle. Preservation strategies include:

- preserve the technology used to create or store the records,
- emulate the technology on new platforms,
-

- migrate the software necessary to retrieve, deliver and use the records,

- migrate the records to up-to-date formats, and
- convert records to standard forms.

Specific Details of Migration Plan (add your plan specs here or attach)

> See the Plan’s checklist (see Appendix A) to ensure required aspects of a migration plan are included. The plan must ensure uniform integration with current platforms and/or supporting software, that accessibility and readability verification steps are performed on the source application, the new source application and any archived applications.

Preservation Plan:

List the best practices your local government will employ to ensure creation of stable records, retention of those records as required, and preserve authenticity of those records.

Records Creators/Preservation Plan Creators

Records or Data Owner Name and Title	**Signature**	**Date**
Records or Data Owner Name and Title	**Signature**	**Date**
Records or Data Owner Name and Title	**Signature**	**Date**
Records or Data Owner Name and Title	**Signature**	**Date**
IT Administrator or Manager Name and Title	**Signature**	**Date**

Governance --- APPROVAL

Name/Title	Signatures	Approved	Dis-Approved	Date
County Commissioners		□	□	
Records Manager		□	□	
LGRC		□	□	
Historical Society (HS)		□	□	

Appendix B: Template 2

IMPLEMENTATION AND MIGRATION PLAN TEMPLATE
(PROJECT NAME)
LOCAL GOVERNMENT NAME
DEPARTMENT NAME
DATE

PURPOSE: The purpose of the Implementation and Migration Plan is to communicate how the project design will be deployed, installed, and transitioned into operation.

[This section should provide a detailed description of both the implementation steps, migration steps from project team to operation team, as well as specific requirements and responsibilities of all involved.]

DESCRIPTION OF IMPLEMENTATION: The implementation of the project consists of the steps involved in the deployment and installation of the project's product either to the customer or throughout the organization it was designed for.

[This section should provide a detailed description of the implementation steps up until the project's product is to be migrated to the responsible group for continued operations.]

POINTS OF CONTACT: Communicating points of contact for all phases of a project is vital to ensure everyone understands who can address questions or concerns relate to the project.

NAME	ROLE	CONTACT INFORMATION

MAJOR TASKS: Often, major tasks represent tasks which require the greatest level of effort, or contain the greatest risk.

[This section should provide a list of the major tasks for the project, what group or individual is responsible, and a brief description of the task.]

IMPLEMENTATION SCHEDULE: The implementation schedule is used to communicate timeframes for the completion of tasks or milestones to the project team.

Task/Milestone	Scheduled Completion Date

SECURITY: Security is an important consideration throughout project implementation and migration.

[This section should describe all security measures included in the implementation and migration of the project so all stakeholders have a clear understanding.]

IMPLEMENTATION SUPPORT:

[This section should provide a description of the personnel supporting the implementation of the project as well as what type of support they will provide.]

LISTING OF HARDWARE, SOFTWARE, AND FACILITIES

[This section should describe the hardware, software, and facilities required to complete the project.]

PERFORMANCE MONITORING: Performance monitoring is a critical tool for ensuring that the implementation and migration of an IT project was successful.

[This section should describe how this will be accomplished and who is responsible for monitoring performance.]

IMPLEMENTATION REQUIREMENTS:

[This section should provide a list of all requirements, which may include hardware, software, facilities or funding, for a successful implementation of the project.]

LISTING OF RECORDS AND DATA THAT IS NOT MIGRATED:

[This section should describe the records and data that is not migrated and how these records will meet retention, preservation or disposal requirements.]

BACK OUT PLAN: As part of implementation planning, there should be a back out plan to revert to existing systems and processes should the implementation of the new system fail.

[This section should describe the back out plan that will be executed should the implementation fail.]

POST IMPLEMENTATION VERIFICATION: It is extremely important that successful implementation of the project is verified.

[This section should describe how successful implementation will be verified so all project team members and stakeholders understand what constitutes successful implementation.]

SIGNATURES: The completed project should be signed off on by administration, IT and RM staff to ensure full support and implementation.

Appendix B: Template 3

Electronic Records and Data Management Migration Plan Template Checklist

ARM 44.14.101 allows for official records to be maintained electronically, so long as an agency has a migration plan that supports records retention requirements for accessibility, and readability.

A migration plan is an agreement between the business owner and its technology service staff that records, and associated data will be stored throughout its lifecycle.

This checklist provides guidance for migration plan considerations and requirements. While this list may not be all inclusive of the agency's requirements for migration of data, it provides minimum guidelines.

- Declare Agency Name, Program Name and Program Code (if unknown, contact SOS-RIM at 444-9000).
- Declare, by position title or work unit, as to who owns the records and data.
- Declare technology being used, by application name(s)
- Declare technology being used, by format type(s)
- Declare that the agreement ensures migration from:
    - one application to its newest version
    - one application to another application in its newest version
- Declare migration timeline (beginning-end)
- Declare how migration accuracy and completeness will be measured

- Declare who performs migration and their roles and responsibilities:
    - Business Owner
    - Information Technology Staff
    - Declare how legacy records and data, that are not migrated, will meet retention, preservation or disposal requirements.
- Obtain Business Owner and Information Technology staff's signature, by position title, as to who has authority over this migration process.