CITY OF Billings

June 2021

ADMINISTRATIVE ORDER NO. 147

Pursuant to the authority granted to the City Administrator in BMCC, Section 2-300, I hereby establish the following procedures regarding:

"ELECTRONIC SIGNATURES AND DOCUMENTS POLICY"

PURPOSE

The City of Billings utilizes modern electronic technology to further efficient and effective delivery of services to the public. This policy for the City has been developed to:

- Promote efficiency in order to conserve public resources;
- Establish guidelines for the use of electronic signatures for certain City transactions;
- Provide reasonable assurance of the integrity, authenticity, and nonrepudiation of electronic documents when electronic signatures are used by the City; and,
- Determine the scope of the City's use of the current electronic signature provider DocuSign as the approved method for affixing an electronic signature to an electronic record. These policies will apply to any future replacement of the DocuSign platform.

Reducing the City's reliance on paper-based transactions will further improve information security and sharing, allow faster approval of and access to documents, and reduce costs and environmental impact. Streamlining the processes described herein that require wet signatures and replacing them with electronic signatures, when practicable, is consistent with the intent of Montana State law to promote electronic transactions and remove barriers that might prevent the use of electronic transactions by governmental entities.

POLICY

1. The City encourages electronic transactions and the use of electronic signatures, and recognizes electronic signatures as legally binding and equivalent in force and effect as a wet signature.
2. The City authorizes the use of the DocuSign electronic signature platform, or any future replacement of such platform, to affix electronic signatures to City records.
3. The City Administrator, Assistant City Administrator, City Clerk, City Attorney, Purchasing Agent and their designees are authorized to use the DocuSign electronic signature platform or any future replacement of such platform to affix electronic signatures to City records as provided in this policy.
4. The DocuSign electronic signature platform, or any future replacement of such platform, is authorized to affix electronic signatures to the following records: Minutes of City Council Meetings, Resolutions and Ordinances Adopted by the City Council, Claim Vouchers Approved by the City Council, and any and all contracts and agreements to which the City is a party.
5. Electronic signatures may be used on City records requiring execution by a third party.
6. Electronic signatures cannot be applied using another employee's name. Records signed on behalf of the City Administrator, Assistant City Administrator, City Clerk, City Attorney or Purchasing Agent by a designee shall use their own electronic signature.
7. An electronic signature is an acceptable substitute for a wet signature on records requiring the signature of any record whenever the use of a wet signature is authorized or require, except as provided herein.

8. If an electronic signature is used for interstate transactions or for documents required by the US Federal government, the electronic signature shall comply with the requirements of the Electronic Signatures in Global and Electronic Commerce Act.
9. This policy in no way affects the City's ability to conduct a transaction using a physical medium and shall not be construed as a prohibition on the use of wet signatures.
10. Documents fully executed in accordance with this Policy shall be considered the original document for the purpose of complying with records retention practices and requirements under the City's retention schedules.
11. It is the responsibility of the City Clerk or the initiating department to retain and store signed documents in accordance with the requirements detailed in the City's records retention policy. Records shall be maintained in a manner that is safe, reliable, and easily accessible in the course of business.

RETENTION

All records creators need to be aware of and implement preservation programs to meet legal and administrative requirements for records management. Digital preservation (for short or long-term) will be the only way to ensure records endure and can be accessed when needed.

All records creators must familiarize themselves with and abide by the Digital Records Creation and Preservation Guidelines for Local Government, by the Montana State Archives and Local Government Records Committee. More information may be found at: https://sosmt.gov/records.

This policy applies to all City employees and governs all uses of electronic signatures and electronic records used to conduct the official business of the City.

All other City policies and procedures shall apply. Personnel will govern themselves in a manner consistent with the Code of Ethics, City Codes and Resolutions. Those who fail to comply with these procedures may be subject to disciplinary action.

Dated this 6/23/2021

DocuSigned by:
Chris Kukulski
57F140BA3A90465...
Chris Kukulski, City Administrator

References:

Digital Records Creation and Preservation Guidelines for Local Government, by the Montana State Archives and Local Government Records Committee

EXHIBIT A

The full Digital Records Creation and Preservation Guidelines for Local Government by the Montana State Archives and Local Government Records Committee may be found at:

https://sosmt.gov/wp-content/uploads/digital-records-guidelines-final.docx

More information may be found at the Montana Secretary of State – Local Government Records Committee website at:

https://sosmt.gov/records/local-committee/#formsd2e3-0aef

Digital Records Creation and Preservation

Guidelines for Local Government

Montana State Archives
and Local Government Records Committee
November 2020

Table of Contents

INTRODUCTION

This document provides guidelines to local government entities regarding the effective creation and preservation of digital records, whether born-digital or digitized copies originally created in an analog format (e.g., paper or photos). All records creators need to be aware of and implement preservation programs to meet legal and administrative requirements for records management. Digital preservation (for short or long-term) will be the only way to ensure records endure and can be accessed when needed.

This document provides considerations for digital preservation which is defined as "as interlocking system of polices, workflows, technical solutions, and *good enough* efforts meant to keep digital objects (files, data, images etc.) authentic and usable in the long term". [1] These guidelines will cover preservation best practices including file formats, file naming, storage, digitization workflow, and preservation planning, all important considerations when building a strong digital preservation plan.

Digital preservation plans for electronic records will have four goals:

Accurate and trustworthy records

[1] From "Planning and Implementing a Sustainable Digital Preservation Program", Erin Baucom. ALA Library Technical Reports.

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 Local Government entities that create or digitize and store their own digital records. The guidelines are only one of many related resources available, 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.

DIGITAL PRESERVATION BEST PRACTICES

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".

MCA/ARM guidance

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 appropriately.

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 and/or reference the resources provided below.

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. Best practice guidelines describe four main types of metadata—descriptive (description of digital object—content), administrative (rights, creator, authenticity), technical (how to access), and structural (how object relates to other objects). 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:

For long-term to permanent records, best practices advise derivatives to be created for use, and a master file be safely stored to ensure access should the derivative become corrupted. Just as local governments were once responsible for safe storage of microfilm, they are now responsible to ensure 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 (or if not possible, use ubiquitous well supported formats) to save records on secure/stable media (preferably dedicated servers rather than temporary media like external hard drives),
- 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. file storage server's mean time between replacements and mean time between failure rating)
- determine a favorable cost/benefit ratio for the best storage options possible, 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 is 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.

Note that the best options may include all or only some of these options. To date migration is the considered the best option, but other options may occur in the future, thus requiring continuing review of this document and future preservation actions.

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 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 C: 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 D: 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 roles including 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.

DocuSign

Certificate Of Completion

Envelope Id: C83C4D09577243FBB215A2FFE9FA3AC8 Status: Completed

Subject: Please DocuSign: 2021 Electronic Signatures Policy AO.pdf, MT Digital records guidelines final ...

Source Envelope:

Document Pages: 41 Signatures: 1 Envelope Originator:

Certificate Pages: 5 Initials: 0 Liz Kampa

AutoNav: Enabled kampal@billingsmt.gov

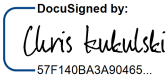
EnvelopeId Stamping: Enabled IP Address: 161.7.22.107

Time Zone: (UTC-08:00) Pacific Time (US & Canada)

Record Tracking

Status: Original Holder: Liz Kampa Location: DocuSign

6/11/2021 5:25:17 AM kampal@billingsmt.gov

Signer Events	Signature	Timestamp
Chris Kukulski kukulskic@billingsmt.gov City Adminisrator City of Billings Security Level: Email, Account Authentication (None) **Electronic Record and Signature Disclosure:** Accepted: 6/23/2021 12:25:11 PM ID: 1dbabac8-ff36-422b-978a-6a2aeefb285a	DocuSigned by:  57F140BA3A90465... Signature Adoption: Pre-selected Style Using IP Address: 161.7.41.49	Sent: 6/11/2021 5:28:08 AM Resent: 6/22/2021 10:49:01 AM Resent: 6/23/2021 9:43:18 AM Viewed: 6/11/2021 10:05:46 PM Signed: 6/23/2021 12:25:33 PM
Denise Bohlman bohlmand@billingsmt.gov Carahsoft OBO City of Billings Security Level: Email, Account Authentication (None) **Electronic Record and Signature Disclosure:** Not Offered via DocuSign	**Completed** Using IP Address: 161.7.26.37	Sent: 6/23/2021 12:25:35 PM Viewed: 6/23/2021 12:26:27 PM Signed: 6/24/2021 7:35:17 AM

In Person Signer Events	Signature	Timestamp

Editor Delivery Events	Status	Timestamp

Agent Delivery Events	Status	Timestamp

Intermediary Delivery Events	Status	Timestamp

Certified Delivery Events	Status	Timestamp

Carbon Copy Events	Status	Timestamp

Witness Events	Signature	Timestamp

Notary Events	Signature	Timestamp

Envelope Summary Events	Status	Timestamps
Envelope Sent	Hashed/Encrypted	6/11/2021 5:28:08 AM
Certified Delivered	Security Checked	6/23/2021 12:26:27 PM
Signing Complete	Security Checked	6/24/2021 7:35:17 AM
Completed	Security Checked	6/24/2021 7:35:17 AM

Payment Events	Status	Timestamps

Electronic Record and Signature Disclosure

ELECTRONIC RECORD AND SIGNATURE DISCLOSURE

From time to time, Carahsoft OBO City of Billings (we, us or Company) may be required by law to provide to you certain written notices or disclosures. Described below are the terms and conditions for providing to you such notices and disclosures electronically through the DocuSign system. Please read the information below carefully and thoroughly, and if you can access this information electronically to your satisfaction and agree to this Electronic Record and Signature Disclosure (ERSD), please confirm your agreement by selecting the check-box next to 'I agree to use electronic records and signatures' before clicking 'CONTINUE' within the DocuSign system.

Getting paper copies

At any time, you may request from us a paper copy of any record provided or made available electronically to you by us. You will have the ability to download and print documents we send to you through the DocuSign system during and immediately after the signing session and, if you elect to create a DocuSign account, you may access the documents for a limited period of time (usually 30 days) after such documents are first sent to you. After such time, if you wish for us to send you paper copies of any such documents from our office to you, you will be charged a $0.00 per-page fee. You may request delivery of such paper copies from us by following the procedure described below.

Withdrawing your consent

If you decide to receive notices and disclosures from us electronically, you may at any time change your mind and tell us that thereafter you want to receive required notices and disclosures only in paper format. How you must inform us of your decision to receive future notices and disclosure in paper format and withdraw your consent to receive notices and disclosures electronically is described below.

Consequences of changing your mind

If you elect to receive required notices and disclosures only in paper format, it will slow the speed at which we can complete certain steps in transactions with you and delivering services to you because we will need first to send the required notices or disclosures to you in paper format, and then wait until we receive back from you your acknowledgment of your receipt of such paper notices or disclosures. Further, you will no longer be able to use the DocuSign system to receive required notices and consents electronically from us or to sign electronically documents from us.

All notices and disclosures will be sent to you electronically

Unless you tell us otherwise in accordance with the procedures described herein, we will provide electronically to you through the DocuSign system all required notices, disclosures, authorizations, acknowledgements, and other documents that are required to be provided or made available to you during the course of our relationship with you. To reduce the chance of you inadvertently not receiving any notice or disclosure, we prefer to provide all of the required notices and disclosures to you by the same method and to the same address that you have given us. Thus, you can receive all the disclosures and notices electronically or in paper format through the paper mail delivery system. If you do not agree with this process, please let us know as described below. Please also see the paragraph immediately above that describes the consequences of your electing not to receive delivery of the notices and disclosures electronically from us.

How to contact Carahsoft OBO City of Billings:

You may contact us to let us know of your changes as to how we may contact you electronically, to request paper copies of certain information from us, and to withdraw your prior consent to receive notices and disclosures electronically as follows:
To contact us by email send messages to: kampal@billingsmt.gov

To advise Carahsoft OBO City of Billings of your new email address

To let us know of a change in your email address where we should send notices and disclosures electronically to you, you must send an email message to us at kampal@billingsmt.gov and in the body of such request you must state: your previous email address, your new email address. We do not require any other information from you to change your email address.

If you created a DocuSign account, you may update it with your new email address through your account preferences.

To request paper copies from Carahsoft OBO City of Billings

To request delivery from us of paper copies of the notices and disclosures previously provided by us to you electronically, you must send us an email to kampal@billingsmt.gov and in the body of such request you must state your email address, full name, mailing address, and telephone number. We will bill you for any fees at that time, if any.

To withdraw your consent with Carahsoft OBO City of Billings

To inform us that you no longer wish to receive future notices and disclosures in electronic format you may:

i. decline to sign a document from within your signing session, and on the subsequent page, select the check-box indicating you wish to withdraw your consent, or you may;

ii. send us an email to kampal@billingsmt.gov and in the body of such request you must state your email, full name, mailing address, and telephone number. We do not need any other information from you to withdraw consent.. The consequences of your withdrawing consent for online documents will be that transactions may take a longer time to process..

Required hardware and software

The minimum system requirements for using the DocuSign system may change over time. The current system requirements are found here: https://support.docusign.com/guides/signer-guide-signing-system-requirements.

Acknowledging your access and consent to receive and sign documents electronically

To confirm to us that you can access this information electronically, which will be similar to other electronic notices and disclosures that we will provide to you, please confirm that you have read this ERSD, and (i) that you are able to print on paper or electronically save this ERSD for your future reference and access; or (ii) that you are able to email this ERSD to an email address where you will be able to print on paper or save it for your future reference and access. Further, if you consent to receiving notices and disclosures exclusively in electronic format as described herein, then select the check-box next to 'I agree to use electronic records and signatures' before clicking 'CONTINUE' within the DocuSign system.

By selecting the check-box next to 'I agree to use electronic records and signatures', you confirm that:

- You can access and read this Electronic Record and Signature Disclosure; and
- You can print on paper this Electronic Record and Signature Disclosure, or save or send this Electronic Record and Disclosure to a location where you can print it, for future reference and access; and
- Until or unless you notify Carahsoft OBO City of Billings as described above, you consent to receive exclusively through electronic means all notices, disclosures, authorizations, acknowledgements, and other documents that are required to be provided or made available to you by Carahsoft OBO City of Billings during the course of your relationship with Carahsoft OBO City of Billings.