110 Horizon Drive, Raleigh, NC 27615
919.459.2081

Electronic Records Preservation

(First draft, September 19, 2018)

www.pria.us

Disclaimer: This is a proposed-for-adoption draft.
There are still known deficiencies in format which PRIA's Style Committee will clean up following final approval.

PROPERTY RECORDS INDUSTRY ASSOCIATION

Copyright Notice, License, Disclaimer
For
Incomplete Work

September 2018

A. **COPYRIGHT NOTICE**: Copyright © 2018 – Property Records Industry Association ("PRIA"). All rights reserved.

B. **LICENSE:** This draft document (the "Incomplete Work") is made available by PRIA to members and the general public for review, evaluation and comment only. This document is under development and not a final version.

PRIA grants any user ("Licensee") of the Incomplete Work a worldwide, royalty-free, non-exclusive license ("License") to reproduce the Incomplete Work in copies, and to use the Incomplete Work and all such reproductions solely for purposes of reviewing, evaluating and commenting upon the Incomplete Work. NO OTHER RIGHTS ARE GRANTED UNDER THIS LICENSE AND ALL OTHER RIGHTS ARE EXPRESSLY RESERVED TO PRIA. Without limiting the generality of the foregoing, PRIA does not grant any right to: (i) prepare proprietary derivative works based upon the Incomplete Work, (ii) distribute copies of the Incomplete Work to the public by sale or other transfer of ownership, or (iii) display the Incomplete Work publicly. Comments on the Incomplete Work must be sent to PRIA.

Any reproduction of the Incomplete Work shall reproduce verbatim the above copyright notice, the entire text of this License and the entire disclaimer below under the following header:

This document includes Incomplete Works developed by PRIA and some of its contributors, subject to PRIA License. "PRIA" is a trade name of the "Property Records Industry Association." No reference to PRIA or any of its trademarks by Licensee shall imply endorsement of Licensee's activities and products.

C. DISCLAIMER: THIS INCOMPLETE WORK IS PROVIDED "AS IS." PRIA AND THE AUTHORS OF THIS INCOMPLETE WORK MAKE NO REPRESENTATIONS OR WARRANTIES (i) EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE OR NON-INFRINGEMENT; (ii) THAT THE CONTENTS OF SUCH INCOMPLETE WORK ARE FREE FROM ERROR OR SUITABLE FOR ANY PURPOSE; AND, (iii) THAT IMPLEMENTATION OF SUCH CONTENTS WILL NOT INFRINGE ANY THIRD-PARTY PATENTS, COPYRIGHTS, TRADEMARKS OR OTHER RIGHTS. IN NO EVENT WILL PRIA OR ANY AUTHOR OF

Contents

Introduction

The increasing use of electronic records since the late 1990s has provided unlimited access and unparalleled retrieval speeds along with new risks and liabilities. Those same electronic records may be the most challenging type of record that recording jurisdictions have been tasked with preserving permanently, i.e., forever. History has shown that preserving recorded documents is a low priority. Preserving electronic records is complex and requires a greater commitment and effort than previous formats and media. This paper addresses the complexity of the issues surrounding preservation of electronic records.

An effective electronic records preservation program should include four vital components:

1. The ability at any time to confirm the existence of a record
2. The ability to authenticate the record
3. The ability to maintain file uniformity or track acceptable file formats, and
4. The ability to recover the authentic record if it has been lost or corrupted.

This PRIA Work Product describes key characteristics of these four components and identifies various strategic layers of insurance that should be considered in an electronic records preservation program.

Although this document is prepared by the Property Records Industry Association for stakeholders in that industry, the information contained in this work product will have application to stakeholders in other industries interested in electronic records preservation.

The History and Evolution of Records Preservation

Paper

In the beginning, there was paper. The paper used for recording real property transactions in the United States was originally manufactured in England beginning in the 15th century. The strength and durability were well known and state archivists recommended or required its use for permanent records.

Photostats

In the early 1920s, typewriting gradually replaced the handwriting of property ownership details. Also, in the early 20th century, a photographic process emerged that could produce an image (copy) of a document. In the 1940s the Photostat machine found its way into county recorder offices. Improved efficiency was the primary appeal to adopting this new technology, but little was known about the longevity of Photostats.

Microfilm

The adoption of microfilm by county recorders began in the mid-1950s. As with Photostats, convenience and efficiency were the primary drivers. Reduced storage space and rapidly improving retrieval technology were compelling reasons for using microfilm rather than creating books.

Although microfilm standards were developed, adoption by recorders was limited. Much of the film was created by untrained staff and/or indifferent vendors. This produced film with poor to average image quality which was often kept in poor storage conditions. As a result, the history of U.S. land recordings is deteriorating, is difficult to migrate to modern formats, and apparently, not worth saving by those who should fund their rescue.

Electronic Images

By the early 1990s, network technology was rapidly evolving to support the bandwidth needs of developing scanning and storage systems. By the mid to late-1990s, TIFF Group 4 had become the "de facto" file format and compression standard for electronic images.

The cumulative impact that imaging and Internet access had on the use of microfilm, both for viewing and for preservation, was devastating. Traditional microfilm companies tried to buck the trend but the promise of improved image quality, streamlined workflow, and instant access made microfilm seem primitive and undesirable.

In 1995, Eastman Kodak Company, recognizing the displacement of film, introduced the Kodak Archive Writer as a way of incorporating the preservation benefits of film into the workflow of an electronic system. Archive Writers attached a Land Records Management System (LRMS) network and used LED to record images on microfilm. Archive Writers have been successfully integrated into many LRMS products and, when their use complies with PRIA's *Recording Electronic Images on Roll Microfilm*[1], the film is customized for preservation and efficient document recovery.

[1] PRIA Resource Library

Preservation Expectations

Recorded real property documents are regarded by recorders as "permanent records[2]." Permanent records are documents that retain legal, historical, and administrative value without any timeframe limitations. A frequently cited assumption is that permanency equates to 500 years in the future; however, 500 years is not forever. The need to migrate image and index data has always been a necessary component of a permanent records preservation strategy.

Achieving 100 percent document existence and authenticity forever is undeniably ambitious and even more so with the multiple media, both analog and electronic, used today to preserve permanent records. The difficulty in attaining this goal was underestimated in the analog world of paper and microfilm as we now understand the consequences of inattention and deferred maintenance. Permanently preserving books, microfilm, and electronic data/images, in such a way as to be absolutely certain that all of the records are being securely maintained and no changes are occurring, is a big burden. It takes great commitment on the part of the recording jurisdiction to establish the appropriate business processes necessary r to achieve and maintain such a high standard of preservation.

The improved quality and performance from the modern LRMS convey the impression that the sophistication of this technology has finally eliminated the need to attend to the health of the records these systems manage. This belief could not be further from the truth. The virtual nature of electronic data, along with the evolving hardware and software that surrounds it, creates a more challenging preservation environment. To be successful, seemingly redundant practices will need to be implemented. These practices should be periodically reviewed for their availability and effectiveness over the lifetime of the records' existence. Together, these practices create layers of insurance to safeguard the health and preservation of electronic records.

There is industry-wide agreement that preservation begins at capture. Image capture most frequently takes place within hours of the act of recording. Capturing the best version of the document is critical and time sensitive for proper preservation. The importance of capture cannot be underestimated, therefore, the people doing the image capture should be focused, well trained and suited for this particular job. Frequently the people handling image capture do not meet these criteria, which is evident in historical document collections across the country.

Local or state laws and regulations often set policies and expectations for permanent retention. These laws and regulations are often slow to be changed. For example, some jurisdictions are still required to keep paper copies of the recorded document, while the majority of jurisdictions are permitted to rely upon microfilm; only a handful are permitted to rely upon electronic images. Potential local disasters (fires, snow, floods, and hurricanes) are seldom addressed when describing acceptable permanent retention options.

[2] State Chart on Permanent Records

Layers of Insurance

Is 100% protection of document preservation possible? Will newer computer operating systems and software somehow reduce the loss or corruption of electronic images?

Preservation is best accomplished using a diverse mixture of record retention strategies. The expenditure of funds on these "layers of insurance" may give the appearance of wasteful redundancy but they are necessary to create a robust preservation and recovery program that ensure the permanency of the public record. Diverse practices create confidence in the recovery process.

The first step in establishing a robust recovery and preservation program is to communicate the responsibilities of a recorder to preserve and maintain forever the existence and integrity of the land records to all of the stakeholders. Stakeholders include IT staff, funding agencies, elected officials/CEO, title professionals, the staff in the recorder's office, as well as the public.

Preservation Roadmap

For preservation layers to be effective, whether a single layer or multiple layers are utilized, business processes need to be established. The business processes become the roadmap that describes in depth how the preservation of the records will be accomplished. In a typical recording preservation environment, this roadmap should include periodic assessment of books and microfilm and routine auditing of electronic records to ensure that the layers are intact and meeting data recovery expectations, and that there have been no unexpected changes. The roadmap should also contain an accurate description of the various media and what periods of time they cover. Finally, the roadmap describes the order in which the various media will be accessed in order to recover missing data/images.

Paper

For centuries, paper was the only medium for recording, accessing and preserving records. High quality paper served all of the recorder's needs and, because of its proven longevity, could be considered one layer of insurance. There are a few states that still require recorders to print out their recorded documents onto paper and put them into bound books. This requirement results in growing storage space issues but bound books are another form of backup that is analog. As long as there is not a fire, flood, insect infestation or other disaster that can destroy the paper, then it is a useful preservation medium (see Appendix 1).

Microfilm

Recorders also use microfilm as a preservation medium which has been an industry standard that requires simple equipment to access. It is important that the conversion to microfilm takes place before any corruption of the electronic images occurs. This form of preservation medium is yet another analog version that can be viewed by either a microfilm reader or other magnifying device. While basic microfilm readers are getting harder to find, newer readers are available that scan the film to a PC for display on a computer screen. Today's electronic technology has improved microfilm's usefulness by presenting a better-quality image in a more organized manner. This benefit occurs when the image is first electronic and then placed on microfilm or when an image is retrieved from existing microfilm. Microfilm can last for hundreds of years if film processing and storage standards are met. If

these standards and preservation practices are not met, microfilm is vulnerable to vinegar syndrome, redox, and mold.[3]

Optical Media

Optical media include the wide variety of CDs and DVDs which developed since the 1980s. These media were used in some recording jurisdictions to store electronic images and data. Optical media are less expensive than creating microfilm and take up less space than paper bound books and microfilm. However, the quality of the media varies widely, especially considering the timeframe during which it was manufactured. Most optical media were expected only to have a life of up to 10 years, which does not meet the "forever" expectation for land records. Where and how the media were stored also impacts the length of time that the contents might remain unchanged. An additional caution is that optical media are susceptible to scratches and fingerprints, making reliable information extraction a challenge. Finally, the equipment and software to read the media, and thus use its content, may not be available long term. These optical media might well disappear much as VHS tapes did. If a recording jurisdiction has optical media, the media may provide yet another layer of insurance in a land records preservation business process as long as its limitations are well understood.

Electronic Systems

With the rise of electronic systems, access to index data and images has significantly improved. The trend toward managing records in a computer system introduced a set of under-appreciated risks that support the need for a "layers of insurance" data recovery practice.

Some of these risks include:

- Computer system failures, including hardware and software, resulting in a loss of data and images.
- Reliance on software that fails to detect corruption or lacks quality control to identify missing images.
- Data or image loss when migrating between systems, performing software updates, or doing general maintenance.
- Inadequate ability to recover corrupted or lost data and images.
- Malicious and innocent alterations, and procedural failures from internal or external sources.
- Procedural failures because of lack of compliance or inadvertent destruction.

In the relatively short time that these electronic systems have been in place, there have already been instances where information has been lost and only recovered by rescanning these records from bound books or preservation microfilm. Had these analog media not existed or been discarded, the lost data and images could not have been recovered without relying on private sector business partners like title plants. It must be noted that not every state allows title plants to operate. Recovering data from a private sector source should only be considered as a last resort.

One benefit of electronic records is that backup copies are made as a standard practice. Although these backup copies serve as an additional layer of insurance, they do not, on a standalone basis, meet

[3] See Appendix 3

all the technical criteria to provide electronic records preservation. This issue is discussed later in this paper.

In an increasingly electronic recording environment, who is responsible for the existence and authenticity of recorded information? Will electronic information and formats survive as well as their analog predecessors? Who governs the security of the database? And, who is responsible for the security to prevent tampering of these documents by hackers?

In summary, electronic records preservation will involve the use of a variety of layers of insurance to protect the existence and integrity of electronic data and images. Records custodians must analyze potential risks of loss and develop a plan that addresses each potential loss. Thought should be given to future technology obsolescence. Forms of redundancy should be developed to protect against any eventuality. These are all issues that must be considered and discussed with answers documented with your vendors and computer department staff.

Offsite Preservation Strategies

Storing electronic data and images is relatively easy and can be cost-effective but does have some important caveats to be considered. As an example, the preservation of electronic data and images involves more than the typical IT process of making backup copies. Backup copies are just one component of a preservation strategy. A thoughtfully designed strategy, that ensures that data and images do not change, is a crucial consideration.

Offsite storage is an essential strategy for records preservation. It should be included in the permanent records preservation plan, as well as for disaster recovery, as evidenced by the many jurisdictions that store backup copies of microfilm offsite.

Whether across town, in another part of the state, or across the country, as the custodian of the public's records, storing a copy of the records away from the location of daily operation is a mission critical part of a preservation strategy. The location and distance to the offsite storage facility should consider the types of disruptions or disasters common to the geographical location. In determining the offsite strategy, other relevant issues include multiple layers of insurance using suitable diverse geographic locations.

With paper and microfilm, offsite storage can be challenging. There are important environmental storage conditions that need to be maintained for the successful long-term preservation of the records. The cost can be a challenge but it is a burden that jurisdictions must find a way to fund.

Most commonly, an offsite facility is going to be provided by a private sector organization. When there is an office disaster, quick and easy access is needed. During research for offsite preservation opportunities, consider ease of access and security. The security considerations include those of the storage facility itself (both physical and environmental), as well as the secure access by the office team. A memo of understanding, or a more detailed contractual agreement, is an important part of storing records in an offsite facility.

In this age of technological innovation, the use of "the cloud" could be a viable off-site storage solution for electronic records if it was constructed in a secure, trustworthy, and regionally diverse environment. The use of off-site preservation strategies, including a qualified cloud solution, are part of an overall electronic preservation strategy that will be addressed in the next section.

Electronic Preservation

Why is electronic preservation important? As jurisdictions reduce their reliance on paper records and microfilm, the electronic data and images become the primary source for daily use and preservation.

Electronic data and images have provided efficiencies for daily use but the efforts and concerns about using them for preservation have just begun to be addressed.

Preservation of electronic data and images may encompass a series of strategies and processes involving multiple devices and media.

Causes of Data Loss

Data loss probably will occur at some point. Each jurisdiction needs to formulate strategies to eliminate (or at least minimize) the potential loss. Here are industry-recognized categories for data losses.

Malicious or Criminal Attack

- Computer virus – a malicious software program that results in data loss or modification over time and use
- Unauthorized access – loss or modification of data without proper authority, e.g., datamining, data manipulation

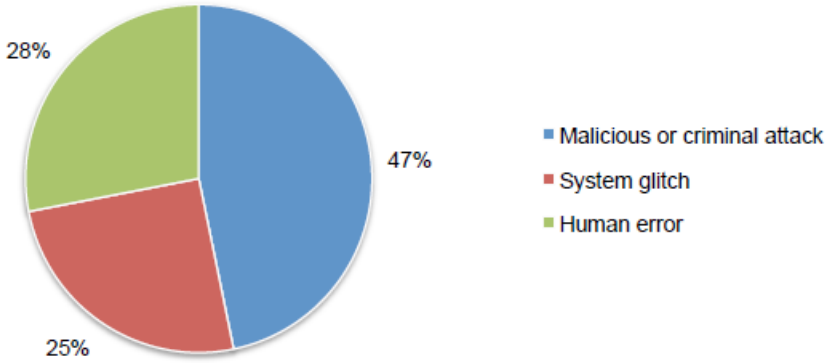
System Glitch

- Hardware malfunction – any failure of the hardware that results in data loss over time and use
- Software corruption – any change in the software that results in data loss or modification over time and use
- Natural disaster – any uncontrollable eventuality that results in data loss or modification
- Bit rot – eventual degradation of storage media that can result in data loss over time and use

Human Error

- Any accidental or malicious action by a person, or persons, that results in loss or modification of data

A key role of electronic records preservation is to address recovery strategies for these and any other unforeseen data loss, all in an effort to protect the existence and integrity of the original record.



Source: "2017 Cost of Data Breach Study" Ponemon Institute, June 2017

Preservation v. Backup

Backup, as performed by information technology staff or vendors, is primarily intended for disaster recovery and not preservation. A disaster recovery process may not recover 100 percent of lost information while a preservation strategy does.

The traditional electronic backup process only allows for current replacement in case of disaster. Questions to be considered:

- How frequently are back-ups made?
- What is the recovery strategy if there is a failure between backups?
- Are the backups being re-used and re-written on top of each previous backup?
- How many of these backups are there that are sequential?
- Are there one, two or three versions or should there be one per quarter and one per year that are kept aside and not written over to preserve a point in time?
- How long will it take to restore operations if recovery is needed?

These are necessary questions to consider when you don't know when the actual corruption occurred. If you are only doing daily or monthly backups, you won't have a complete electronic record which captures data and images from six months ago, much less two years ago, or whenever the corruption might have occurred. Corrupt data and images might not be evident for months or years into the future.

Additional concerns include the change of servers and/or the change of operating systems on both servers and computers. Here are other considerations:

- Will the backups from two years ago still be accessible or useable with the current operating system?
- Is the current version of software you are using compatible with backups from several years ago?
- Did the tape drive or other form of backup capture all data and images and can they be imported back into the current system three to ten years later?
- Has the integrity of the data been compromised due to the passage of time?

Traditional business continuity is based on two fundamental objectives:

- Recovery Point Objective (RPO) – the maximum targeted period during which data and images might be lost because of a service interruption or major incident. Should computer operations suddenly be interrupted or cease, what is the maximum possible time where data and images might be lost? Is this acceptable? If not, you need to establish an objective that is acceptable. This current potential loss is usually determined by the time interval between data backups or between when "database images" are created. If backups are made daily, you could lose up to 24 hours-worth of data, i.e., all the data since the prior day's backup. If "database images" are created every 15 minutes, you could lose up to 15 minutes-worth of data and images. If a backup is being written to another server instantaneously, you may not lose anything as long as both the primary and the backup systems are not affected at the same time. How much time is acceptable? This is your RPO.
- Recovery Time Objective (RTO) – the targeted maximum period before operations return to a state of normalcy after a service interruption or major incident. If there is a service interruption, how long will it take for IT to restore operations? This recovery period will vary based on the type of service interruption. How much recovery time is acceptable? This is your RTO.

RPO and RTO relate to business continuity, but alone they do not guarantee long-term preservation.

In summary, to understand the requirements for the preservation of electronic documents, the distinction must be established between backup and preservation by Information Technology (IT) personnel and records custodians. Some IT personnel may feel that periodic backups of electronic data constitute a preservation strategy. However, the objectives of these periodic backups may not address the requirements needed for long-term preservation of electronic images and data such as the items addressed above. Traditionally, backups are intended to ensure business continuity and disaster recovery of information and systems within the constraints of the RPT and RTO. These practices may fall short of what is required to address the preservation characteristics presented in this section.

To establish a foundation for preservation, it is important for both recorders and IT to remember that land records are permanent, i.e., they need to be preserved forever. For purposes of this paper the concepts of recovery, retention and preservation are considered to be separate actions. The objectives and practices of traditional IT business continuity plans do not encompass the concept of preservation. IT may presume that backup and preservation are accomplished with the same functionality, but that is not the case.

Electronic Preservation Strategy

An electronic preservation strategy must address all the following requirements:

- Authenticity
    - Stored data and images are vulnerable to accidental or malicious change. Steps should be taken to ensure that these files cannot be overwritten or changed while in the custody of the recorder. Write Once Read Many (WORM) recording would be an example of this type of protection.
- File Integrity

  - Land records are legal documents and, as such, their integrity is essential. An electronic identification process must create a unique "fingerprint" (hash algorithm) of each image as soon as possible after recording. This fingerprint information must be maintained in a safe but accessible location to be used as a baseline value for future comparison to ensure the veracity of the image. The hashing calculation should be strong enough that duplicates are not possible.
- Archival auditing
  - The electronic fingerprinting process (described above) must be periodically run against every stored image over its lifetime. The result from each run must be compared to the file's baseline value to assure its existence and authenticity.
- Data existence
  - With or without warning, hardware or software malfunction can render stored data irretrievable. If the auditing process discovers a difference between the baseline fingerprint value of a file and its current value, the system must report the discrepancy to the responsible parties. The system should be self-auditing and self-reporting.
- Recoverability
  - A process must be in place to restore lost data and images to their original, authentic condition. A credible restoration process ensures that lost or corrupted files can be recovered. The system should be self-correcting.
- Versioning
  - When stored data and images are legitimately corrected, those corrections should be tracked through a versioning process that documents the file's history of modification. Versioning should meet audit guidelines applicable to the jurisdiction.
- File uniformity
  - Awareness of the file types being stored, along with the contents (e.g., compression, header data and associated metadata) is important to ensuring their long-term preservation, and is critical for a complete and reliable data migration.
  - Various electronic image formats have been adopted and used over the years during which electronic images have been created. As of March 2017, PRIA recommends the use of PDF/A-2A as a standard for preservation of electronic images.[4] Other preservation format standards may evolve.
  - Computer systems and software continue to evolve at a rapid pace. Expecting new systems to maintain backward compatibility with historical media and data formats has already proven to be problematic. Insisting on backward compatibility would eventually limit the technological progress that we have come to expect. When information access, migration, and/or preservation are at stake, it is incumbent on the person(s) with custodial responsibility of that information to recognize looming hardware and/or software obsolescence and make the necessary changes to avoid orphaning image and/or index data.
- Life Expectancy (LE)
  - LE refers to the timeframe during which information can be retrieved without significant loss of data and image integrity. Implied in an LE rating is both existence and access.

[4] See PRIA March 2017 TIFF-PDF/A White Paper.

For example, information written on polyester base microfilm, processed correctly, and stored at 21˚C and 50 percent relative humidity has an LE of 500 years. This means that the information the microfilm holds is expected to be retrievable for 500 years after processing. At this time, there is no LE rating associated with electronic storage media or the data it holds.

- Data migration
  - Whether technology obsolescence or improved performance is the impetus to migrate, changing storage media or data format is inevitable during the lifetime of a permanent record collection. For a migration program to reliably move information, it needs to recognize every data format in the source file (see File Uniformity). Even when this is done, files can become corrupted during the transfer process so comparing the migrated file with the original is a necessary audit procedure to ensure that the migration was successful.

Conclusion

Preserving electronic records is a complex undertaking. It requires vigilance, and a greater commitment and effort than was practiced with previous preservation formats and media. This paper addresses these electronic records preservation issues and offers the following conclusions:

- Land Records are permanent (forever) in all United States jurisdictions. Forever is a long, long time. Permanent records are documents that retain legal, historical, and administrative value without any timeframe limitations. Responsibility for permanency rests on the shoulders of the current records custodians and their successors.
- Jurisdictions (both public and private) must develop an understanding of, and strategy for, electronic records preservation. The difficulty in attaining permanency has been underestimated in the past and will be again with electronic records. Is it acceptable to lose any record at any time?
- The on-going existence and authenticity of land records as captured require continuous attention for effective preservation.
- While laws and regulations, which set records management policies, are often slow to change, new technology options advance rapidly.
- Preservation of electronic records costs money and resources are often not made available. Spending money on preservation has not been a high priority for recording jurisdictions, their larger locale, or private businesses.
- Creating a plan for electronic records preservation is essential. The plan should include viewpoints and expertise of a variety of people with different skill sets and expectations. The principles of preservation need to be considered and incorporated into the plan. Preservation is not computer system backup.
- Previous preservation media (e.g., paper, microfilm, optical media) should be incorporated as possible emergency options for recovery. These prior media are considered layers of insurance. As older layers of insurance become obsolete, new layers need to be added.
- The preservation plan must be regularly reviewed for effectiveness over a record's lifetime, as new technologies may outpace the ability of an office to manage its records resources.

Appendix 1 – Evolution of Paper

PRIA previously issued A Brief History of Records Preservation with more detail on paper records. The graphic below provides a timeline for the evolution of paper.

Appendix 2 - Technical References

LEGAL ADMISSIBILITY

ANSI/AIIM TR31/4-1994 (R1999): Performance Guidelines for Admissibility of Records Produced by Information Technology Systems as Evidence - Part IV: Model Act and Rule

ISO/TR 12036:2000: Micrographics -- Expungement, deletion, correction or amendment of records on microforms

ANSI/AIIM TR31-2004: Legal Acceptance of Records Produced by Information Technology Systems

ISO/TR 12037:1998: Electronic imaging -- Recommendations for the expungement of information recorded on write-once optical media

ISO/TR 12654:1997: Electronic imaging -- Recommendations for the management of electronic recording systems for the recording of documents that may be required as evidence, on WORM optical disk

ISO/TR 15801:2009: Electronic imaging - Information stored electronically - Recommendations for trustworthiness and reliability

MEDIA MANUFACTURING

ISO 18901:2010: Imaging materials -- Processed silver-gelatin-type black-and-white films -- Specifications for stability

ISO 18902:2013: Imaging materials -- Processed imaging materials -- Albums, framing and storage materials

ISO 18902:2007/Cor 1:2009: Imaging materials -- Processed imaging materials -- Albums, framing and storage materials

QUALITY ASSURANCE - RECOMMENDED PRACTICES

ANSI/AIIM TR15-1997: Planning Considerations, Addressing Preparation of Documents for Image Capture

ANSI/AIIM MS44-1988 (R1993): Recommended practice for quality control of image scanners

ISO 10550:1994: Micrographics -- Planetary camera systems -- Test target for checking performance

ISO 6200:1999: Micrographics -- First generation silver-gelatin microforms of source documents -- Density specifications and method of measurement

ISO 12650:1999: Document imaging applications -- Microfilming of achromatic maps on 35 mm microfilm

ANSI/AIIM MS48-1999: Recommended practices for filming public records on silver halide microfilm.

MEDIA AND ENCLOSURE TESTING

ISO 18917:1999: Photography -- Determination of residual thiosulfate and other related chemicals in processed photographic materials -- Methods using iodine-amylose, methylene blue and silver sulfide

ISO 18915:2000: Imaging materials -- Methods for the evaluation of the effectiveness of chemical conversion of silver images against oxidation

ISO 18916:2007: Photography -- Processed photographic materials -- Photographic activity test for enclosure materials

MEDIA INSPECTION

ISO/TR 12031:2000: Micrographics -- Inspection of silver-gelatin microforms for evidence of deterioration

ENVIRONMENTAL CONDITIONS

ISO/TR 18931:2001: Imaging materials - Recommendations for humidity measurement and control.

ISO 18911:2010: Imaging materials -- Processed safety photographic films -- Storage practices

ISO 18934:2011: Imaging materials -- Multiple media archives -- Storage environment

TRUSTED SYSTEM ARCHITECTURE

AIIM ARP1-2007: Analysis, Selection, and Implementation of Electronic Document Management Systems (EDMS)

ISO 14641-1:2012: Electronic archiving -- Part 1: Specifications concerning the design and the operation of an information system for electronic information preservation

Appendix 3 – Sample Electronic Records Policies

Some national and state electronic records policies and recommended practices:

- AIIM ARP-1-2009 - Analysis, Selection, and Implementation of Electronic Document Management Systems (EDMS)
  - https://www.aiim.org/Resources/Standards/AIIM_ARP-1-2009
- California Trusted System Specification
  - http://www.sos.ca.gov/archives/programs/electronic-records/electronic-records-guidebook/trusted-systems
- Florida Electronic Records Policy
  - Rule 1B-26.003 Florida Administrative Code
  - Electronic Records and Records Management Practices (November 2010)
- ISO/TR 15801:2017(en) - Document Management - Electronically Stored Information – Recommendations for Trustworthiness and Reliability
  - https://www.iso.org/obp/ui/#iso:std:iso:tr:15801:ed-3:v1:en
- Washington State Electronic Records Policy
  - http://apps.leg.wa.gov/wac/default.aspx?cite=434-662&full=true