

Digital Imaging Policy

DRAFT

Last Update June 26, 2001

PURPOSE

The purpose of this policy is to establish an imaging policy for all University departments and offices that create, use, and manage digital images.

SCOPE

This policy applies to all digital images created by University personnel within the Indiana University system.

STATEMENT OF AUTHORITY

Authority for this policy is derived from the University groups responsible for the effective management of IU's information resources: the Committee on Institutional Data, the Committee of Data Stewards and the Indiana University Archives. This Committee on Institutional Data is comprised of vice presidents, deans and directors and is charged with establishing overall policy and guidelines for management and access to the institutional data resources of Indiana University. The Committee of Data Stewards is comprised of university and campus officials who have planning, policy and operational responsibilities for the management and use of institutional data. The Data Stewards, as a group, are responsible for recommending policies and establishing procedures and guidelines for university-wide management of institutional data. The University Archives, a division of the Indiana University Libraries, is authorized to establish and promulgate standards, procedures and techniques for the effective management of University records. It is also responsible for preserving the University's documents and records of historical value.

POLICY SUMMARY

The following elements shall be present in an imaging program to ensure the reliability, accuracy, security, and accessibility of the digital images it creates:

- system and procedural documentation that outlines system specifications and describes and defines the creation, maintenance, use, and preservation of digital images within the system
- hardware and software that meet industry standards, and procedures and practices that comply with best practices for managing digital image programs
- training schedules that include an initial training period as well as regular, ongoing retraining in order to ensure that the staff understand the policies and procedures and any changes to these that may occur
- audit mechanisms that monitor the reliability, authenticity and security of scanned images.

ADDITIONAL INFORMATION

Key terms used in this policy are defined in a separate *Glossary of Terms*. Standards and best practices can found in the works listed in the separate *Bibliography*. Additional detail on procedures for interpreting and implementing this policy can be found in a separate set of *Digital Imaging Guidelines*.

POLICY REQUIREMENTS

SYSTEM PLANNING AND IMPLEMENTATION

System Administrator

- University offices planning imaging programs shall identify a person as system administrator to monitor the operation of the program and the training of assigned personnel.

System and Procedural Documentation

- Policies, guidelines, and procedures defining all system implementation activities shall be created and distributed to all personnel involved in the imaging program.
- Specific procedures shall be created for: scanning and entering data; ensuring that all information within images is readable and that the accuracy of index terms is verified; revising, updating and deleting images; backing up disks; establishing and implementing security measures; providing access; and implementing disposition procedures.
- The System Administrator shall be responsible for maintaining and distributing this documentation.

Compliance

- Procedures shall be established to ensure that management practices related to scanned images are in compliance with pertinent laws, regulations and statements of best practice.

Retention and Disposal

- Records created by and stored in an imaging system shall be disposed of only in accordance with an approved retention and disposal schedule.

Business Processes

- IU digital imaging programs shall be integrated into and support the business processes and the workflow environment thereby ensuring that the scanned images are available, understandable and useable.
- Whenever possible, University offices shall create models of business processes to determine which processes the scanned images support and how the images relate to other business records.

Audit Trails

- IU digital imaging programs shall maintain a record of when and by whom scanned images have been created, revised, or deleted.
- IU digital imaging programs shall track access and use of scanned images so as to provide a full, trustworthy audit trail.

Training

- All staff members using the imaging system shall be required to undergo basic training on the system and to pass a scanning quality test before they may add or dispose of records to the official system.

Monitoring

- IU digital imaging programs shall annually review all scanning implementation procedures and guidelines.

Equipment Maintenance

- Digital imaging hardware and software shall be routinely checked to ensure that they accurately and reliably reproduce all original documents, and equipment maintenance logs shall be maintained.

SYSTEM ARCHITECTURE AND IMAGE SPECIFICATIONS

System Architecture

- IU digital imaging programs shall choose a system with "Open System Architecture," which provides users with the most flexibility when choosing equipment and will support interconnection, information system integration, and information sharing.
- If the system under review does not possess open architecture, IU digital imaging programs shall justify why a proprietary system is required and demonstrate how it will interconnect with other systems.

Image Resolution

- When determining document scanning resolution, IU digital imaging programs shall consider data storage requirements, document scanning rates, and the accurate reproduction of the image.
- For good quality images of text documents, IU digital imaging programs shall use a scanning density of 200-300 dpi.
- For "archival" quality images of text documents that must be retained indefinitely, IU digital imaging programs shall use a scanning density of at least 600 dpi.

Image Authenticity/Integrity

- IU digital imaging programs shall ensure that scanned images are protected from accidental or intentional deletion or modification.
- Where data longevity or records integrity is a primary concern, IU digital imaging programs shall use a recording media that is not rewritable.
- IU digital imaging programs shall select equipment that conforms to the standard methodology for media error detection and correction.

Image Metadata/Profiles

- Metadata describing the content and structure of the digital image and its context of creation shall be included within the digital image or linked to it.

Image Security

- IU digital imaging programs shall establish procedures for ensuring that only authorized personnel create, copy, modify, or use scanned images within the system.
- IU digital imaging programs shall develop backup procedures designed to create security copies of scanned images and their related indexes.

Image Access

- IU digital imaging programs shall use an indexing system database that provides for efficient retrieval, ease of use, and up-to-date information on the scanned images stored in the system.

Image Storage

- Digital images shall be saved in non-proprietary file formats, such as ASCII for text or Tagged Image File Format (TIFF) for images.
- Storage media for digital images shall be stored in a controlled environment. Technical specialists recommend a stable environment, with a temperature between 65 and 75 degrees and a relative humidity between 30 and 50 per cent.

Image Compression and Encryption

- If the image file needs to be compressed due to size, IU digital imaging programs shall use standard compression and decompression algorithms.
- IU digital imaging programs shall not utilize encrypted software source code.

Image Preservation/Migration

- IU digital imaging programs shall develop specific plans for an ongoing process of migrating scanned images of continuing value to newer hardware and software and to new storage media.

GLOSSARY OF TERMS

Audit trails: A record showing who has accessed a computer system and what operations he or she has performed during a given period of time.

Compression: Storing data in a format that requires less storage space.

Encryption: The translation of data into a secret code. To read an encrypted file, the user must have access to a secret key or password that enables him/her to decrypt it.

Imaging system: A system used to store information electronically by recording a digital reproduction of a scanned document.

Metadata: Structured data about data. Metadata describes the content and structure of the digital image and the context of its creation. For example, metadata will describe how, when, and by whom a particular set of data was collected and how the data is formatted.

Migration: The process of translating data from one generation of technology to another while maintaining the functionality. Unlike the older strategy known as "refreshing" or the process of copying digital information onto new media, migration addresses both the obsolescence of the storage media and of the hardware/software controlling and managing the digital documents.

Non-proprietary file format: A file format in the public domain, which can be used by anyone without buying a special license.

Non-rewritable media: Media that allows users to write data to it just once and that cannot be erased like conventional magnetic media. An example would be write-once-read-many (WORM) optical disks.

Open system architecture: Software or hardware whose specifications are public, which includes officially approved standards. The great advantages of open systems are that software is portable and scalable and that anyone can develop add-ons for the system.

Record: Evidence of a business transaction.

Resolution: Refers to the sharpness or clarity of an image.

Retention and disposition schedule: Identifies how long records must be retained to satisfy administrative, fiscal, legal, and historical requirements.

Workflow: Workflow is the tasks, procedural steps, organizations or people involved, required input and output information, and tools needed for each step in a business process.

BIBLIOGRAPHY

AIIM TR2-1992, Glossary of Imaging Technology. Silver Spring, MD: Association for Information and Image Management, 1992.

AIIM TR25-1995, The Use of Optical Disks for Public Records. Silver Spring, MD: Association for Information and Image Management, 1995.

AIIM TR26-1993, Resolution as it Relates to Photographic and Electronic Imaging. Silver Spring, MD: Association for Information and Image Management, 1993.

AIIM TR27-1996, Electronic Imaging Request for Proposal (RFP) Guidelines. Silver Spring, MD: Association for Information and Image Management, 1996.

AIIM TR28-1991, The Expungement of Information Recorded on Optical Write-Once-Read-Many (WORM) Systems. Silver Spring, MD: Association for Information and Image Management, 1991.

AIIM TR31-1992, Performance Guideline for Admissibility of Records Produced by Information Technology Systems as Evidence Part 1: Evidence. Silver Spring, MD: Association for Information and Image Management, 1992.

AIIM TR31/2-1993, Performance Guideline for Acceptance of Records Produced by Information Technology Systems by Government Part 2: Acceptance by Federal or State Agencies. Silver Spring, MD: Association for Information and Image Management, 1993.

AIIM TR31/3-1994, Performance Guideline for Admissibility of Records Produced by Information Technology Systems as Evidence Part 3: User Guidelines. Silver Spring, MD: Association for Information and Image Management, 1994.

AIIM TR31/4-1994, Performance Guideline for Admissibility of Records Produced by Information Technology Systems as Evidence Part 4: Model Act and Rule. Silver Spring, MD: Association for Information and Image Management, 1994.

ANSI/AIIM MS44-1988 (R1993), Recommended Practice for Quality Control of Image Scanners. Silver Spring, MD: Association for Information and Image Management, 1993.

ANSI/AIIM MS52-1991, Recommended Practice for the Requirements and Characteristics of Original Documents Intended for Optical Scanning. Silver Spring, MD: Association for Information and Image Management, 1991.

ANSI/AIIM MS53-1993, Standard Recommended Practice - File Format for Storage and Exchange of Images - Bi-Level Image File Format: Part 1. Silver Spring, MD: Association for Information and Image Management, 1993.

ANSI/AIIM MS59-1996, Media Error Monitoring and Reporting Techniques for Verification of Stored Data on Optical Digital Data Disks. Silver Spring, MD: Association for Information and Image Management, 1996.

Cinnamon, Barry and Richard Nees. The Optical Disk-Gateway to 2000. Silver Spring, MD: Association for Information and Image Management, 1991.

D'Alleyrand, Marc R., Ph.D. Networks and Digital Imaging Systems in a Windowed Environment. Boston, MA: Artech House, 1996.

Elkington, Nancy E., ed. Digital Imaging Technology for Preservation: Proceedings from an RLG Symposium held March 17 and 18, 1994. Mountain View, CA: The Research Libraries Group, Inc., 1994.

National Archives and Records Administration. "Digital Imaging and Optical Digital Data Disk Storage Systems: Long-Term Access Strategies for Federal Government Agencies." Washington, D.C. 1994.

National Archives and Records Administration and National Association of Government Archives and Records Administrators. "Digital Imaging and Optical Media Storage Systems: Guidelines for State and Local Government Agencies." Washington, D.C. 1991.

Saffady, William. "Stability, Care and Handling of Microforms, Magnetic Media and Optical Disks." Library Technology Reports, Vol. 27, January/February 1991: 63-87.

Warner, Will. "Special Report: An Introduction to TIFF." Inform, Vol. 5, February 1991: 32-35.