TABLE OF CONTENTS

Superseded by 2003 Revision

Superseded by 2003 Revision

INTRODUCTION

Public officials are responsible by law for ensuring that their records are protected and accessible. This responsibility applies regardless of the records' form or storage media.

These guidelines are for use by public officials in the design of responsible digital imaging systems. The guidelines are advisory in character and are not intended to serve as a rigid set of requirements. National technical standards, established practices, and research in the professional literature form the basis for these guidelines. These guidelines are designed to identify critical issues for public officials to consider in designing, selecting, implementing, and operating digital imaging technologies. These issues are especially important for systems used for mission critical records or for long-term/archival records.

Within these recommendations, digital document imaging is defined as:

> *the conversion, storage, and distribution of information displayed by, but not directly modified by, a computer.*

The recommendations are listed in order of their implementation.

These guidelines are based partly upon the work done by the Alabama Department of Archives and History and published in their technical leaflet *"Guidelines for the Use of Digital Imaging Technologies for Long-Term Government Records in Alabama*." Their recommendations formed the basis for this work and are included here with their permission. We appreciate their expertise and generosity.

Superseded by 2003 Revision

PROJECT PLANNING

RECOMMENDATION 1: PRIOR TO SELECTING A DIGITAL IMAGING SYSTEM, CONDUCT A RECORDS AND WORKFLOW ANALYSIS TO DETERMINE AND DOCUMENT EXISTING AND PLANNED AGENCY INFORMATION NEEDS.

The examination of existing workflow patterns and records is the crucial first step in determining the need for a digital imaging system. A workflow analysis assesses the processes of records creation, access, and retrieval to determine areas where reengineering can improve operational efficiency. This reorganization of business or work processes may be simple or extensive in approach. Implementing a digital imaging system significantly impacts the current work processes because personnel create, retrieve, use, and store documents in a different way. The detail and complexity of the process reengineering affects the project schedule and cost justification.

A records analysis looks at existing operations to determine what records are best suited for digital imaging applications. Digital imaging is primarily an application designed to enhance access to information. Consequently, those records best suited for digital imaging applications are records that have short retention periods (typically less than ten years), are used or viewed by multiple people, have multiple points of access or index fields, or require rapid access.

Digital imaging applications are not designed solely to save storage space, although this is often touted as a selling point for these applications. The use of digital imaging technology to save space assumes the destruction of the original material once scanned. Destruction of original records with records retention periods of less than ten years once reformatted into digital images is acceptable. Destruction of original materials with records retention period greater than ten years once reformatted into digital images should be considered with extreme caution. While many records are destroyed once microfilmed, there are

established microfilming standards, which insure the quality and long term survivability of microfilm if the standards for film production and storage are followed. There are no such standards for images produced by imaging systems. Thus, one must be concerned about the long-term survivability of the data created by a digital imaging system. Considering the continuous state of technological change, any record in an electronic format cannot be considered stable. Hence, the destruction of original materials with retention periods greater than ten years cannot be recommended once those records have been reformatted into digital images.

The State Archives of the Ohio Historical Society can assist in analyzing an agency's record keeping systems. Agencies that are considering imaging records with permanent retention periods must contact the State Archives for a system and records analysis to determine if maintaining the records in an eye readable format is also necessary.

Superseded by 2003 Revision

RECOMMENDATION 2: PRIOR TO SELECTING A DIGITAL IMAGING SYSTEM, CONDUCT A COST BENEFIT ANALYSIS TO DETERMINE THE COST JUSTIFICATION OF A SYSTEM PURCHASE AND TO DETERMINE THE POSSIBLE BENEFITS TO THE AGENCY WITH ITS IMPLEMENTATION.

Cost justifying a digital imaging system allows a financial comparison between the current and proposed record keeping systems to help in making a procurement decision. The cost-justification goal of a digital imaging system is to offset the cost of the equipment and software by reducing personnel and storage costs or allowing the existing staff to process more work through the improvement of work processes.

A typical cost justification includes the following major areas: a study of current operations, a proposed system architecture, equipment pricing, and financial indicators, including payback period, net present value, and rate of return.

To determine a cost estimate, the following components should be considered: system hardware, system software, application software, communications hardware and software, system maintenance, training, project management, facilities upgrades/site preparation, staffing costs, and other miscellaneous costs.

To determine the costs of current operations, the following components should be considered:

Costs of file creation - including paper, folders/filing supplies and labor to create files and insert into filing system

Costs of file maintenance/use - including filing equipment, floor space needed for files (remember to double the space actually occupied by the file equipment), labor to retrieve/copy/refile documents, "wait time" of person requesting the information and the additional costs for lost file search and retrieval

Costs of disposition - including boxes for off-site storage or destruction, off-site storage, destruction, and the labor to move from active to inactive storage/destruction

There may be additional costs that should be added to the appropriate area depending on your agency's particular circumstances (e.g., transportation costs).

SYSTEM SPECIFICATIONS AND SELECTION

RECOMMENDATION 3: REQUIRE AN "OPEN SYSTEMS ARCHITECTURE" FOR DIGITAL IMAGING APPLICATIONS OR REQUIRE VENDORS TO PROVIDE A BRIDGE TO SYSTEMS WITH NON-PROPRIETARY CONFIGURATIONS.

Although the term open systems architecture is defined in various ways, public officials should follow a system design approach that permits future component upgrades with minimal degradation of system functions. This open system architecture allows the system to be upgraded over time without a significant risk of records loss. It also supports the importing and exporting of digital images to and from other sources. One key factor in achieving an open systems architecture is the adoption of non-proprietary standards. The flexibility of an open systems architecture helps enable long-term records to be accessed and transferred from one hardware or software platform to another.

RECOMMENDATION 4: AS RECORD INTEGRITY IS A PRIMARY CONCERN, IT NECESSARY TO USE RECORDING MEDIA THAT ARE NOT REWRITABLE.

When selecting optical storage media, the issues of data longevity and integrity must be considered. There are a variety of optical disks, such as WORM (Write Once Read Many), CD-R (Compact Disk-Recordable) that are not rewritable. These media offer a high level of data security because alteration of data is not achievable without destruction of the media itself. If a record is no longer needed, software may allow the pointer to the data to be disabled, preventing normal access. Because the data cannot truly be deleted, however, it may remain accessible by other means and therefore a potential liability.

RECOMMENDATION 5: USE A NON-PROPRIETARY DIGITAL IMAGE FILE FORMAT. IF USING A PROPRIETARY FORMAT, PROVIDE A BRIDGE TO A NON-PROPRIETARY DIGITAL IMAGE FILE FORMAT.

A digital image file format is a structured container for information about each digital image and the image data. Information about the digital image file includes, but is not limited to, its name, width, length, resolution, and compression techniques. The computer requires this information to interpret the digital image. It is essential to use a non-proprietary image file format to ensure the ability to transfer successfully digital images between different systems or when a system is upgraded or modified.

American National Standards Institute (ANSI)/Association for Information and Image Management (AIIM) MS53-1993, Standard Recommended Practice - File Format for Storage and Exchange of Images - Bi-Level Image File Format: Part I details a standard definition for file formats. Despite the existence of a standard, there is not an agreed-upon, industry-wide image format standard. Many digital imaging systems use the Tagged Image File Format, or TIFF. Because different versions of TIFF exist, there is still no absolute guarantee that images can be transported seamlessly from one system to another. Comprehensive documentation of the digital image file format, including TIFF, is recommended.

A number of other file formats exist, such as Graphics Interchange Format (GIF), Joint Photographic Experts Group (JPEG), and Bitmap (BMP). These file formats are commonly used in conjunction with hypertext markup language (HTML) for Internet and intranet applications. Many systems or third-party graphics packages will convert images from one to another, although often with unpredictable results.

Superseded by 2003 Revision

RECOMMENDATION 6: USE INTERNATIONAL TELECOMMUNICATIONS UNION (ITU) GROUP 3 AND GROUP 4 COMPRESSION TECHNIQUES OR HAVE THE VENDOR PROVIDE A BRIDGE TO THESE TECHNIQUES.

The large file sizes of typical scanned documents require digital image compression to support data transmission and to promote storage efficiency. Today most digital imaging systems use standard compression algorithms to "shrink" images. Standard compression techniques are instrumental in ensuring a migration strategy for records needed for long-term use. Two international standards are currently available. Using compression techniques conforming to either of these specifications will increase the likelihood that the images can be used with other technologies or migrated between systems.

RECOMMENDATION 7: WHEN DETERMINING DOCUMENT SCANNING RESOLUTION, CONSIDER DATA STORAGE REQUIREMENTS, DOCUMENT SCANNING THROUGHPUT RATES, AND THE ACCURATE REPRODUCTION OF THE IMAGE. VALIDATE VENDOR CLAIMS USING A SAMPLING OF THE AGENCY'S DOCUMENTS.

A digitized image consists of black and white dots or picture elements (pixels) measured in dots per inch (dpi). Generally, the higher the number of dpi, the higher the legibility of the reproduced image. Images scanned at higher dpi rates, however, use more storage space on the disk and may require longer scanning times. The selection of scanning density involves a trade-off between image clarity, storage capacity, and speed. When selecting a scanner, ask the vendor to perform a quality test on a broad sampling of documents at various dpi settings so that an appropriate end-to-end throughput rate and resolution can be determined.

For good quality images in scanning modern office records, use a scanning density of at least 200 dpi. A higher scanning density is appropriate for deteriorating documents, and documents with a visual element such as, engineering drawings, maps, documents with background detail or documents that are going to have an Optical Character Recognition program performed on them. The display resolution of the inspection/verification monitor and printer should match the scanning density of the document scanner. When scanning continuous tone images, such as photographs, maps, and illustrations, use gray scale or color imaging technology.

RECOMMENDATION 8: SELECT EQUIPMENT THAT CONFORMS TO THE STANDARD METHODOLOGY FOR MEDIA ERROR DETECTION AND CORRECTION. THE SYSTEM SHOULD PROVIDE TECHNIQUES FOR MONITORING AND REPORTING VERIFICATION OF THE RECORDS STORED ON A DIGITAL OPTICAL DISK, AND THE SYSTEM ADMINISTRATOR SHOULD ACTIVELY FOLLOW THE STATUS OF THE MONITORS.

Digital imaging technology uses two methods within the Error Detection and Correction (EDAC) system to minimize digital image recording and retrieval errors. The first method uses error correction codes to detect and correct data read errors automatically. The second employs correction code software to determine if and when the utilization of error correction codes is approaching a critical point. Monitoring the error correction status information provides an audit trail to measure the progress and degree of disk degradation. Tracking error correction trends will indicate an appropriate timetable for recopying disks.

Superseded by 2003 Revision

The Association for Information and Image Management's (AIIM) Standards Committee has developed a standardized methodology for reporting the error rate data to the operating system for user evaluations. *ANSI/AIIM MS 59-1996, Media Error Monitoring and Reporting Techniques for Verification of Stored Data on Optical Digital Data Disks*, describes these standards.

Another precaution against losing long-term records because of defective disks is to require the use of digital optical disks with a guaranteed minimum shelf life of five years and a minimum post-write life of twenty years.

RECOMMENDATION 9: SPECIFY THAT THE SMALL COMPUTER SYSTEM INTERFACE (SCSI) COMMAND "WRITE AND VERIFY" IS USED WHEN WRITING DATA TO DIGITAL OPTICAL DISKS.

The "Write and Verify" command, available within the Small Computer System Interface (SCSI), is valuable for assessing how accurately the scanned information is transferred from the central processing unit of the computer to the digital optical disk. "Write and Verify" requires verification from the system that the digital image is correctly written to the disk and provides additional protection for continued access to long-term records.

RECOMMENDATION 10: USE AN INDEXING DATA BASE THAT PROVIDES FOR EFFICIENT RETRIEVAL, EASE OF USE, AND UP-TO-DATE INFORMATION ABOUT THE DIGITAL IMAGES STORED IN THE SYSTEM. THE INDEXING DATABASE SHOULD BE SELECTED AFTER AN ANALYSIS OF AGENCY OPERATIONS AND USER NEEDS.

Reliable access to scanned images depends on an accurate, up-to-date index database. Indexing a digital image involves linking descriptive image information with header file information. Normally, index data is manually key-entered using the original documents or the scanned images, either at the time of image capture or later in the production process. Index data verification, in which data base entries are compared with the original source documents for completeness and accuracy, is crucial because an erroneous index term may result in the inability to retrieve related images.

RECOMMENDATION 11: PROVIDE SPECIFIC PLANS FOR AN ONGOING PROCESS OF MIGRATING LONG-TERM AND ARCHIVAL RECORDS FROM OLDER TO NEWER HARDWARE AND SOFTWARE PLATFORMS.

Public officials are responsible by law for ensuring that their records are protected and accessible for the time period stipulated in the records retention schedule. This responsibility applies regardless of the storage media the records are recorded and maintained on. With that responsibility comes the authority for the agency to decide in which medium to maintain their records. Should an agency decide to destroy original records once imaged, that agency must ensure that their long-term and archival records are continually accessible. Systems and physical devices could be operational for ten years or more, but system technology will often be superseded within two to three years. If the system stores records with retention periods exceeding the life span of the hardware and software, it is essential that the administrator plan for future data migration. A migration strategy documents how an organization will transfer long-term and archival records from one generation of hardware and software to another generation without losing system functionality. The strategy should be written and available with current system documentation. It is important to recognize that migration strategies need to be budgeted for in order to insure their success (see recommendation 19).

Superseded by 2003 Revision

Current strategies for migrating digital imaging system records include:

- upgrading equipment and software as technology evolves and periodically recopying disks as required
- recopying optical disks based upon projected longevity and/or periodic verification of the records or
- transferring the data from an obsolete generation of optical disks to a newly-emerging technology, in some cases bypassing the intermediate generation that is mature but at risk of becoming obsolete.

Agencies must submit a revised records retention schedule for records that they are reformatting (i.e. changing medium from paper to digital image). Agencies that are considering imaging records with permanent retention periods must contact the State Archives for a system and records analysis to determine if maintaining the records in an eye readable format (paper, microfilm, etc.) is also necessary.

Superseded by 2003 Revision

SYSTEM IMPLEMENTATION

RECOMMENDATION 12: ASSIGN A PERMANENT STAFF MEMBER AS SYSTEMS ADMINISTRATOR AND REQUIRE THE VENDOR TO PROVIDE A PROJECT DIRECTOR DURING THE INSTALLATION AND TRAINING PERIODS.

The assignment of a qualified staff member, preferably with systems administration experience, is critical to the effective implementation and maintenance of a digital imaging system. The systems administrator should be responsible for overall project management, and the development and maintenance of written system documentation which describes the requirements, capabilities, limitations, design, operation, and maintenance of the digital imaging system. Making a vendor representative responsible for installing the equipment and training the systems administrator and other appropriate agency staff will help to ensure successful implementation of the system.

RECOMMENDATION 13: ESTABLISH OPERATIONAL PRACTICES AND PROVIDE TECHNICAL AND ADMINISTRATIVE DOCUMENTATION TO ENSURE THE FUTURE USABILITY OF THE SYSTEM, CONTINUED ACCESS TO LONG-TERM RECORDS, AND A SOUND FOUNDATION FOR ASSURING THE SYSTEM'S LEGAL INTEGRITY.

It is the responsibility of office administrators, rather than vendors and manufacturers, to maintain written documentation of system procedures, also called Standard Operating Procedures or SOPs, including access and security policies and procedures. Security and access policies should be developed to protect the system and the records from alteration or unauthorized use.

It is important to maintain a written record of procedures, operating systems, decisions, changes and updates made to the system. It should be a complete, specific, and updated on a regular basis. Documentation of operating procedures should include a description of methods for scanning or entering data and revising, updating, or expunging records, hardware and software operating manuals, indexing techniques, backup procedures for disks, tapes, microfilm, etc., procedures for testing the readability of records, security safeguards to prevent tampering and unauthorized access to protected information as well as the disposition of original records.

Technical Documentation should include:

Hardware - types, brand names, model numbers, and dates of installation of all hardware components of the system.

Software - version numbers, implementation dates, and backup copies of all systems software and applications programs.

Maintenance - an equipment maintenance log should be kept to document the occurrence of regular maintenance

In regard to legal admissibility and trustworthiness, records stored on a digital imaging system should be treated no differently than records stored on magnetic disk or tape. The key is for the systems administrator to become familiar with how the rules of evidence apply to such records. Procedural controls should be established and followed to protect the integrity of the records.

These procedural controls should be documented and should reflect requirements for the legal acceptance of records as outlined in *AIIM TR31-1992, Performance Guideline for the Admissibility of Records Produced by Information Technology Systems as Evidence*. This AIIM performance guideline stresses the importance of specifying the processes used to create the records, demonstrating that records are produced and relied upon in the regular course of business, establishing quality control and audit procedures, conducting formal training programs, and providing written documentation for each procedure. Case histories indicate that system requirements for good archival maintenance are consistent with the requirements for the admission of records under the "rules of evidence" laws. Records Administrators should be familiar with how the rules of evidence apply to Ohio's public records. Policies and procedures should be followed to protect the integrity of long-term records.

Superseded by 2003 Revision

RECOMMENDATION 14: INSTITUTE PROCEDURES TO ENSURE QUALITY AND INTEGRITY OF SCANNED IMAGES.

Scanning of Records

At the beginning of a shift, or every day, verify each image scanned until accuracy of the scanner settings is determined. Visual quality evaluations of one hundred percent should be performed at the time of new installation or upgrades in software or hardware, or when new operators or projects begin. These evaluations can be reduced as confidence is met.

Data Integrity

Data integrity of digital records should include procedures for regular inspection of the images and system components to insure both short and long term accessibility. Create a schedule of how often inspections of digital records and hardware and software should be made. These procedures should also include inspection of digital images to confirm that the optical drive, storage media, and other system components are working properly.

At least annually, inspect a sampling of images from both primary and backup storage media to verify continued accessibility. Data maintained on electronic media should be copied onto new media at regular intervals.

Audits

Audit procedures should include schedules for regular, special, and annual inspections. Each audit should produce a written report detailing when it was performed, the name of the auditor, and the findings.

On a regular basis, or at least every six months, a sampling of recorded images should be retrieved from the storage media and displayed for inspection to confirm that the optical drives, storage media, and other system components are working properly.

Special audits should be performed at the time of new installations or when upgrades are made to the hardware or software, or when determined by staff or users.

At least annually, perform a more thorough audit to answer whether procedures are in place and documented in writing and whether operators are following the procedures. Include an evaluation of the outputs of the digital records and an evaluation by the user(s).

RECOMMENDATION 15: DESIGN BACKUP PROCEDURES TO CREATE SECURITY COPIES OF DIGITIZED IMAGES AND THEIR RELATED INDEX RECORDS.

For this recommendation, backup is defined as *the short-term copying or duplication of an information base, including the operating system, the applications, the active data and image sets.*

The purpose of backup is to provide replacement of data or images lost due to system or user error, or in the event of a disaster. In terms of imaging, this is especially vital, as the original paper-based information may no longer exist. In this event, without a backup, image may not be restored. Creating a duplicate copy of records in another format or another system is an effective method of ensuring access to long-term information. Backup copies also support system integrity and legal admissibility requirements.

Backup (and more importantly restoration) of data requires the following to be strictly enforced:

- A written, documented procedure for backups
- Regular audits of that procedure, to determine validity and completeness of data and images to be restored.

Documentation must include:

- Complete step-by step instructions for performing the backup
- If the backup is automated, instructions for both setting up the automated sequence and ways to manually bypass automation if needed
- Complete instructions for implementing backup solutions, including hardware and software
- A chart which includes:

  A schedule showing normal start time and estimated time frame
  Types of backups performed (examples are full, incremental, differential)
  Examples of logs generated by the process and/or the application
  Complete instructions for performing both partial and complete restore from any point in the process.
  As part of the documentation, all of these steps should be checked for accuracy

Audits can be performed by either internal or external personnel on a regular, scheduled basis. They should be based solely on the documentation provided, and can only be certified if the documentation is correct.

Backups, in general, should allow for disaster recovery. In other words, they must be constructed in such a way that data can be retrieved no matter what the circumstances. There are two ways of ensuring this:

Superseded by 2003 Revision

- Duplicate backups being done at more than one site--in the event of a disaster, backups should be available at the other site(s). This allows backups to be done remotely without human intervention at each site.
- Backups can be immediately moved to an offsite location--in the event of a disaster, the backup can be retrieved. In this case, human intervention is required.

RECOMMENDATION 16: PROVIDE ADEQUATE ENVIRONMENTAL CONDITIONS FOR THE DIGITAL OPTICAL DISKS.

Even in an optimum environment, digital optical disks are susceptible to deterioration. Adverse storage conditions, especially high humidity, can cause rapid deterioration of the media. A prudent storage guideline for digital optical disks is to adhere to the temperature and humidity levels recommended for magnetic media storage. Technical specialists recommend a stable environment, with a temperature between 65 and 75 degrees, and a relative humidity between 30 and 50 per cent. Digital optical disks should never be stored in direct sunlight nor placed near sources of heat.

Dust, debris, and fingerprints affect digital optical disks. Plastic cartridges should never be removed; nor should the cartridge shutter be opened to expose the digital optical disk's recording surface. To protect disks from warping, they should not be subject to pressure and should be stored in an upright position when not in the disk drive.

Agency officials should request that the vendor supply specifications for the storage of digital optical disks and ensure that office conditions meet these specifications during installation of a system.

RECOMMENDATION 17: THE RETENTION AND DISPOSAL OF ELECTRONIC IMAGES AND ELECTRONIC RECORDS SHOULD BE INCORPORATED INTO AGENCY RETENTION SCHEDULES.

Record Disposal is the destruction of a record by whatever means necessary and appropriate to insure that it is un retrievable by any known manual or technological method.

When deleting digital images, agencies should assure that the images are actually erased from the storage media. Deleting files commonly only deletes the file reference and location information, not the file itself. Agencies should work with vendors and Information Technology personnel to insure that files are deleted completely. Once a record is destroyed, remember to destroy duplicate copies from system backups, redundant and secondary archive copies.

RECOMMENDATION 18: A DISASTER PREPAREDNESS PLAN IS PARAMOUNT TO A PROPERLY CREATED SYSTEM OF IMAGE AND DATA BACKUP, STORAGE AND RECOVERY.

A Records Disaster is a sudden and unexpected event that results in loss of records or information essential to an organization's continued operation. Types of disasters include the obvious: fire, windstorm, flood, and earthquake. Less obvious disasters include vandalism, unauthorized access, loss, theft, equipment failure, leaking pipes, insects, rodents and mold.

The effects of disaster on digital document imaging systems can be more easily controlled than on paper, due to the ease of duplication and portability of the media. A disaster preparedness plan should include

Superseded by 2003 Revision

preparation for any disaster natural or otherwise which effects would be to render the organizations information stored in the Digital Document Imaging System permanently un-retrievable.

A proper plan should include provisions for the off-site storage of index data, digital images, and system documentation, proper security for back-up media, a destruction schedule for back-up media, an image and data recovery plan, and a plan for routine system audits.

An off-site facility for the purpose of storing the back-up media must be identified. This site should be physically removed far enough from the host site to protect it from the effects of the same disaster experienced at the host site. The facility should be accessible 24 hours per day, 7 days per week. Proper security measures must be put in place to protect the contents of the back-up media from access by unauthorized personnel.

A schedule of retention and destruction of index data and digital images should be maintained for the backups. This schedule should be identical to the schedule for the original media.

Provisions for image and data retrieval from back-up media should be established. This may include either hiring a contractor to provide the services or having your own redundant system available.

The same individuals who would be responsible during an actual disaster should perform a routine audit of the image and data recovery process. This audit should include test retrievals from backup/stored media.

For vital records, agencies might consider creating a Hot or Redundant Site. Vital records are those records considered essential for the ongoing business of an agency and without which the agency could not continue to function effectively. A Hot Site is a second physical location housing a completely operational retrieval system. The purpose of the Redundant Site is to provide facilities for immediate retrieval of document images no longer available at the host site due to disaster. This site should be physically removed far enough from the host site to protect it from the effects of the same disaster experienced at the host site while maintaining reasonable access for audits, backups and Disaster Recovery events.

All hardware and software at the redundant site must be kept current and compatible with the host system. The most critical areas are the media drives for the index data and the document images. Examples of software would include the operating system (Microsoft Windows 98), Tape Drive software, Optical Disk Drive Software, Application Software (Minolta, Filenet, OTG).

All documentation available to users at the host site should be duplicated and made available at the Hot Site. This includes hardware manuals, software documentation, procedures etc.

The same individuals who would be responsible during an actual disaster should perform a routine audit of the Disaster Recovery System. This audit should include test retrievals from the Hot Site or user site if connectivity is provided for in the Preparedness plan.

Proper facilities must be provided if instantaneous access by multiple users is necessary immediately following a disaster. Most importantly, a connection between the user network and the redundant digital imaging retrieval system must be established.

Superseded by 2003 Revision

RECOMMENDATION 19: BUDGET ANNUALLY BETWEEN FIFTEEN AND TWENTY PER CENT OF THE ORIGINAL SYSTEM ACQUISITION COST FOR UPGRADES, TRAINING, AND MAINTENANCE.

Administrative managers should be aware of the high cost of maintaining and upgrading digital imaging systems. Unless these costs are factored into the continuing support of system maintenance and improvement, the system is in danger of becoming obsolete and requiring a far greater cost outlay to restore its effectiveness. Also, records stored in an outdated system tend to be at greater risk than those in a well-supported system. Continued planning and budgeting for the migration of long-term and archival records, as discussed in Recommendation 11, is essential for the success of any digital imaging project.

IF YOU NEED ASSISTANCE

The State Archives staff of the Ohio Historical Society provides assistance to state and local government agencies regarding the records administration considerations affecting the design and implementation of digital imaging systems. Direct questions or comments concerning digital imaging technologies to:

Charles Arp
Assistant State Archivist
Ohio Historical Society
1982 Velma Avenue
Columbus, Ohio 43211-2497
carp@ohiohistory.org
(614) 297-2581

For more information about scheduling records, contact your agency's records manager.

Superseded by 2003 Revision

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.

Superseded by 2003 Revision

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.

Superseded by 2003 Revision