DIGITIZATION OF DEPARTMENTAL RECORDS

No: SAAP 13-2

Date: April 24, 2013

Authority: Wisconsin Statute § 16.61
Wisconsin Administrative Rule 12
UWM Administration

Initiator: Provost

Responsible Party: Information Technology Policy Committee

Digitization, or digital imaging, is an increasingly popular strategy for departments and offices looking to manage their records. When implemented appropriately, digitization can dramatically improve access to records while simultaneously reducing the need for physical records storage space. However, digitized records introduce new responsibilities, costs, and challenges not present in management of paper records. These guidelines are intended to help UWM departments determine if digitization of their records is an appropriate course of action, and if so to assist them in developing a secure and robust digital imaging program and associated processes.

1. DEFINITIONS

- **a. Digital Imaging System:** A system (including people, machines, methods of organization, and procedures) which provides input, storage, processing, communications, output, and control functions for digitized representations of original public records.
- **b. Public Records:** Documents used by offices and individuals to conduct business on behalf of UWM and the State of Wisconsin. Public records are fully defined in state law by Wis. Stat. § 16.61(2)(b) and may not be destroyed without permission.
- **c. Open Records Request:** A request made by a member of the public to a state unit (including UWM) to make available certain public records. All public records are potentially subject to disclosure through Open Records requests, with some exceptions. See: Wis . Stat. 19.31-19.39.
- **d. Records Retention and Disposition Authority (RRDA):** Legal document issued by the Wisconsin Public Records Board which defines records series and provides guidelines for their retention and disposition (destruction or transfer to Archives).
- **e. Open Systems Architecture:** Systems design that defines interface standards and permits the interconnection of system elements provided by many vendors.
- **f. Authenticity:** a quality of electronic records that indicates accordance with the original document and verifies that the record has not been significantly altered post-creation.
- **g. Source File:** The copy of the digital image initially created by scanning tools and used for creation of subsequent preservation or access copies.
- **h. Convenience copy:** a copy of the digital image intended for use by the office or individual. These copies are not intended for long-term preservation and are usually not required to be managed according to public records laws.

i. **Metadata:** Information associated with digital images that describes the content and structure of the document and its context of creation.
j. **Migration:** The process of converting a digital image to a more recent file format and/or moving it to a newer computer or file system to help prevent obsolescence of the image.
k. **Document Scanning Resolution:** The level of clarity at which a document is scanned, usually measured in Dots Per Inch (DPI) or Pixels Per Inch (PPI). High-DPI documents will be clearer but the file size will be larger.

2. LEGAL ISSUES AND RECORDS MANAGEMENT

Records maintained within a digital imaging system are subject to open records requests under Wis. Stat. 19.31-19.39, and must be producible on short notice as required. Failure to produce records under this law may be cause for legal action. Wisconsin Administrative Code Ch. Adm 12 outlines six properties that public records in electronic format must maintain:

- **Accessible:** the record must be able to be located and retrieved in a reasonable amount of time.
- **Accurate:** the record must correctly reflect the original record when displayed on a retrieval device or reproduced on paper.
- **Authentic:** the record reflects the creator's input and can be substantiated.
- **Reliable:** the record correctly reflects the initial record each time it is produced by the system.
- **Legible:** The characters within a record can be identified to the exclusion of all other characters.
- **Readable:** The characters within a record are recognized as words, complete numbers, or symbols.

Records stored within digital imaging systems must be managed according to Wisconsin Stat. § 16.61, which requires Records Retention and Disposition Authorities (RRDAs) to be in place for any and all records series created and maintained in the course of University business. RRDAs define a record series, provide a retention period for that series, and give instructions for records disposition (destroy, destroy confidentially, or transfer to Archives). It is recommended that records with temporary disposition (i.e. those not scheduled for transfer to the Archives or other permanent retention) be destroyed upon or shortly after expiration, in order to protect records integrity in the event of a security breach.

A partial list of UWM and UW-System RRDAs that apply to campus offices may be found at http://www4.uwm.edu/libraries/arch/recordsmgt/common.cfm. If no RRDA exists for a given records series, contact UWM Records Management to have a schedule created. See http://records.uwm.edu for additional information.

3. NEEDS ASSESSMENT AND COST ANALYSIS

Before embarking on a digitization program, departments should assess whether digitization is an appropriate solution for their records management needs. In general, digitization is best implemented in cases where quick, simultaneous, and/or distributed access to records is necessary for fulfillment of a department's responsibilities, or when such access would significantly increase the efficiency of a department's operations. Digitization is generally NOT an appropriate solution for reducing storage costs, as the cost of hardware, software, storage space, training, and maintenance of systems can greatly exceed the cost for storing those same records in paper form.
Some of the factors that must be evaluated during an initial needs assessment include:

- **Program Purpose:** Why is the digitization program being undertaken? Will digitized records be maintained in lieu of or in addition to paper records?
- **Business Process Evaluation**: how does the digitization program improve business processes?
- **Information Security:** What security precautions must be taken to protect digitized records?

- **Amount and Accumulation:** How many records are to be digitized? What is the estimated rate of addition per year to these records?
- **Type of Record:** What type of document (textual, photograph, map, etc.) is to be digitized? How does that affect the need to provide additional information about the records?
- **Records Retention:** How long must digitized records be retained? Are the records scheduled under a current Wisconsin Records Retention and Disposition Authority (RRDA)?

For a cost analysis, some of the factors to consider include:

- **System Hardware and Software**
- **Image Management Application**
- **Facilities Upgrades/Site Preparation (**including additional storage space)
- **Project Management**
- **Training**
- **Staffing**
- **Ongoing Maintenance, Support, and Upgrade** (generally about 10-20% annually of initial implementation cost)

If a cost analysis does not yield a net benefit for a digitization program, consider retaining files in paper form in your office, or explore storage alternatives (off-site storage, etc.). See also UWM Records Management Guideline #2, Offsite Records Storage:
http://www4.uwm.edu/libraries/arch/recordsmgt/guideline2offsite.cfm

4. SYSTEM SPECIFICATIONS AND SELECTION

Due to the broad scope of most digitization projects, departments are strongly encouraged to select a reliable vendor for scanning of records and management of digitization systems. This selection should be pursued through UWM's normal procurement channels in consultation with Purchasing and UITS, as detailed at http://www4.uwm.edu/bfs/procedures/purch/. RFPs for Digital Imaging Systems should include, at minimum, the following requirements:

- **Open systems architecture**, including non-proprietary compression standards. This type of 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. If proprietary standards or architecture are unavoidable, the vendor should provide a bridge to systems with non-proprietary configurations and/or license the software beyond the length of the contract.
- **Specifications for hardware/software that will require vendors to support and maintain their product(s).**
- **Controls and system auditing tools.** Effective audit trails can automatically detect who had access to the system, whether staff followed existing procedures, or whether fraud or unauthorized acts occurred or are suspected.
- **Image authenticity/integrity tools.** The system should ensure that the images are protected from accidental or intentional modification. Equipment should also conform to methodology for media error detection and correction.
- **Records management system integration.** System records should be linked to approved RRDAs and retention periods and include provisions for automatically or manually purging records beyond their scheduled retention dates. See Records Management, below.
- **Appropriate document scanning resolution.** Consider data storage requirements, document scanning rates, and the accurate reproduction of the image. See Technical Specifications, below.
- **Access to records.** Systems should 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. The

index storage method should be based on standard relational database technologies with access using standard SQL queries. See Metadata Integration, below.

- **Appropriate levels of security.** Systems should ensure that only authorized personnel are able to create, copy, modify, or use scanned images within the system. Different types of scanned records may include different security requirements. See Information Security, below.

5. TECHNICAL SPECIFICATIONS

Digitization technologies allow offices to control the resolution, size, color, bit-depth and other qualities that affect how the image appears on a computer screen or is output to a printer. Furthermore, once captured, a digital image can be saved in numerous file formats that may or may not include compression technologies that reduce the file size of the file. Choices offices make in these areas need to be cost-effective while still producing an accessible, accurate, authentic, reliable, legible, and readable record throughout its life cycle.

Convenience copies, those that are not used for preservation but to be used in the office, may be of more diverse formats and resolutions in order to best fit the needs of the office. The office, for example may wish to create JPG or PDF files from the source files that are of lesser resolution and are compressed for day-to-day use.

6. INFORMATION SECURITY AND TRAINING

Departments should appoint a staff member, preferably one with systems administration experience, as the administrator of any digital imaging system. This 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. All other personnel to be given access to the system should undergo comprehensive training on the system before being granted privileges to add or dispose of records. For security reasons, only personnel who require access to digitized records for their daily job duties should have access to the digital imaging system.

Before creating any digital imaging system, Departments should also consult with UWM Information Security to assess their data classification and determine any additional security needs. See http://infosecurity.uwm.edu for additional information.

7. DOCUMENT SCANNING PROCESS

Prior to scanning, documents to be imaged should be arranged in such a way that the organization of those documents is clearly discernable. Office personnel in charge of scanning or coordination with scanning vendors should also prepare documents for efficient processing (remove staples, unfold paper, remove extraneous documents, etc.). For the sake of consistency and security, employees responsible for scanning should be specially designated and trained for this purpose.

Once scanning has completed, digital images should be inspected by the system administrator or other responsible party to ensure the accuracy, legibility, and readability of the documents. In cases of scanning projects with very large numbers of documents, a visual quality evaluation of a sample of documents may be appropriate.

8. METADATA INTEGRATION

Metadata is information associated with digital images that describes the content and structure of the digital image and its context of creation. To increase the accessibility and ease of retrieval of digitized files, metadata should be included within records or linked to them for this purpose.

The creator(s) of the records to be digitized should work with the digitization system administrator and/or vendors to determine what metadata is necessary for appropriate indexing and retrieval of records. A workflow to add this metadata to records at the point of digitization should also be created. Where appropriate, records creators should use controlled vocabularies to increase accessibility and group like documents together.

9. STORAGE AND MIGRATION

It is recommended that source files of digitized records be stored on a network server or as part of an enterprise-wide document management system and NOT on removable media. Appropriate campus IT staff must be notified if the official copy of any public record is to be stored on campus servers, in order to determine storage and security requirements. If, for whatever reason, it is not possible to preserve source records on a server, it is recommended that these records be stored on removable WORM (write once, read many: e.g. CD-R, DVD-R) discs only. Rewritable media are generally unacceptable storage media for digitized records because they do not preserve the authenticity (fixity) of records. At least 2 copies of each disk should be made and kept in separate, secure, locations. Be sure to label external storage media with particular care since it is impossible to determine content merely by looking at a disk or tape.

Digital Imaging Systems which contain records with retention periods longer than 5 years should include provision for migrating records, i.e. converting images and indexes to newer file formats or storage media to prevent hardware or software obsolescence. A migration strategy will document how a department 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.

10. FOR MORE INFORMATION

Records Management: http://records.uwm.edu
Information Security: http://infosecurity.uwm.edu
Legal Affairs: http://www4.uwm.edu/legal/
Purchasing: http://www4.uwm.edu/bfs/depts/purch/

Sources: UW System; Harvard University "Guidelines for Scanning University Records"; UW-Madison "ARMS Bulletin #7"; Indiana University "Digital Imaging Policy";State of Georgia "Electronic Document Imaging Systems Guidelines"; Kansas State Historical Society "Digital Imaging Guidelines"; Minnesota Historical Society "Digital Imaging"; New York State "Guidelines for Ensuring the Long-Term Accessibility and Usability of Records Stored as Digital Images"