UW Scanning Requirements

Scanning or Imaging is the process by which paper documents are copied and saved as digital images - usually PDF (preferred) or TIFF files. Scanning paper records **does not** automatically authorize the destruction of the source documents from which the scanned images have been created. Only if your office writes a Scanning Policy that meets the UW Scanning Requirements and has it approved by Records Management Services can the electronic record can legally take the place of the paper document.

The requirements which follow are based on Imaging Systems, Standards for Accuracy and Durability – Chapter 434-663 of the Washington Administrative Code (WAC). These requirements must be met to justify the use of scanned images as official replacements for the original paper records.

To begin writing a Scanning Policy for your office or department, we recommend you schedule a consultation with UW Records Management Services at the beginning of the process, before records are scanned. Please contact us at 543.0573 or urc@uw.edu.

Records Retention

All records have a specific amount of time they must be maintained. This specific amount of time is called a "retention period". Retention periods are based on the content of a record. Retention periods are found on a tool called a Records Retention Schedule. Retention periods included in Records Retention Schedules apply to all records regardless of their physical form or characteristics.

Like all electronic records, scanned files **must** remain accessible and readable for their full retention period. This includes finding the file, opening the file, and reading the file regardless of the software used in its creation. Paper records scanned according to an approved scanning policy can be destroyed immediately after confirming that they were scanned successfully.* It is important to note, however, that the retention period which would have been applied to the paper record must instead be applied to the scanned record.

** If you are being audited or have received notice of an audit, if there is litigation regarding the records (or even pending litigation), or if there is a public records request, the original paper records should not be destroyed until the matter is resolved and the destruction hold is lifted, even if you have scanned them according to an approved scanning policy.*

Technical Scanning Requirements

- Any kind of record can be scanned including color text documents, photographs, and maps, plans, and engineering drawings.
- Black and white, gray, and color paper records can be scanned.
- Scanners must be set at a minimum of 300 dpi (dots per inch).
- It is recommended that scanned records be saved as PDF files. If records are scanned using a mobile device, JPEGs are an acceptable format.

Quality Control

- Scanned document images must be inspected visually to ensure they are complete (the entire document has been captured), clear, and easily read.
- The number of original paper pages must be compared to the number of scanned pages to ensure that every page was scanned.
- It is highly recommended that each scanned record be visually inspected to ensure that the image is complete, clear, and usable. If necessary scanned records should be compared to the original paper document to ensure accuracy.
- At a minimum, high volumes of scanned documents can be reviewed in batches through a process called Sampling. When employing sampling, every tenth document is visually reviewed to ensure the scanning quality is consistent and the images are clear and usable.

Image Enhancement

There are times when there is a problem with the final scanned image that makes it difficult to read and less than usable. If the scanned document is to replace the original paper record these common problems must be corrected:

- Speckles or spots on the scanned image: clean the glass on the scanner and rescan the paper.
- Skewed images that are not properly aligned: rescan the paper so that the image appears straight. All portrait orientation pages should be rotated to read from left to right. All landscape orientation pages should be rotated with the top of the page facing the left.
- Only part of the document is captured by the scanner: rescan the paper so that it is properly aligned and the entire page is included in the scanned image.
- The scanned record is of poor quality and is not clearly readable: reset the dpi (dots per inch) setting on the scanner to a setting higher than 300 dpi and scan again. Keep increasing the dpi until the record is as readable as possible.
- Sometimes the condition of the original paper record precludes a good quality scanned image from being produced. In these cases it is necessary to document the problem to avoid future confusion over the poor quality of the scanned image. There are several different ways this can be accomplished:
    - Keep the paper copy of the records that did not scan well; or
    - Tag the image in metadata as “best scan possible” (Use Acrobat Pro “Additional Metadata” in the Document Properties description tab); or
    - When indexing/naming the document include, “best scan possible”.

Managing Scanned Records

Organizing and Filing Scanned Records

The strategy which will allow scanned records to be identified for destruction at the end of their retention period must be determined at the beginning of the scanning process. The strategy begins with how the scanned records will be filed.

Scanned records can be saved to a file/directory based system like a networked drive or similar storage location (e.g. I-drive), or scanned records can be saved to a database, or in a document/content management system. Scanned records should not be saved to thumb drives or to the hard drive (e.g. C-drive) on a personal computer.

Networked Drive or Storage Location

While a networked drive or storage location (e.g. I-drive) is not a preferred method for saving (individually or collectively) large amounts of scanned records, it can be useful for saving basic business records like receipts, meeting minutes, and timesheets.

If saving to a networked storage location (e.g. I-drive):

- Establish a file plan/structure for the drive/directory that will hold the incoming records. Know how much information is coming in and plan for how much additional information will be stored over time.
- Save individual documents to folders. Include the year the records were either created or received in the folder title.
- Consider using or including the formal record series title as found on a UW records retention schedule in the folder title.
- Consider using Acrobat Pro “Additional Metadata” in the Document Properties description tab to create background information on the document.

Databases and Document/Content Management Systems

Because of the amount of metadata that can be stored with the image, a database or document/content management system is the preferred method for saving large quantities of scanned records as well as records which are frequently searched.

If saving to a database:

- Configure the database or system so that records with the same retention are mapped.
- Include identifying retention information in the metadata of the record.
- Know how often the data will be searched and what criteria will be used. The criteria used for searching data will form the basis for metadata tags.

Suggested metadata tags for an image include:

- Original Document Date
- Document Type
- Cut-Off /Expiration Date (the date that triggers the count down on the retention period)
- Retention Period
- Keywords
- Index ID information (student number, budget number, EID, subject identifier, etc)
- “Best Scan Possible”

Modifying Scanned Records

It is important to ensure that the original content of a scanned record is **not altered or modified** once it has been finalized. Scanned records should be “read only” to ensure that there is no improper alteration or modification.

However, many times it is useful to add a note on a PDF using a text box. This is not considered a modification of the scanned record and is an acceptable and practical way to make notes on an electronic record.

Migration and Preservation Strategies

Archival records and records with a retention period of greater than 6 years require a migration and preservation strategy before the original paper documents can be destroyed. This is to ensure the scanned records can be opened and read (remains accessible and readable) for their full retention period. As hardware becomes obsolete and software is replaced by more current versions this can be very difficult to accomplish for records that are considered archival (permanent) or have very long retention periods.

The following steps must be taken when scanning an archival record or records with a retention period of more than 6 years:

- When scanning archival or potentially archival records, the most basic option for preservation is to create microfilm of the scanned records. If produced correctly, microfilm is a proven extremely long term stable option for preservation; or
- Original paper records designated as "**Archival**" on a records retention schedule must be transferred to the University Archives. Contact John Bolcer, University Archivist, for transfer procedures at jdbolcer@uw.edu.
- When scanning records designated as "**Potentially Archival**" on a records retention schedule, contact John Bolcer, University Archivist, to discuss whether the original paper records should be destroyed or transferred to the University Archives.
- When maintaining records with a records retention period of more than 6 years, additional consideration must be applied to the constraints of the system in which they are saved. Anytime newer technologies are implemented (hardware or software) or legacy systems are retired, any electronic records that have not yet exceeded their retention requirements must be migrated to the new platform. New versions of the software cannot be skipped.

Disaster Preparedness and Backups

Scanned records must be backed up to ensure that, regardless of any damage they may sustain for any reason, they remain accessible and readable for their full retention period. The following steps must be taken to ensure adequate back-up of scanned records:

- Back-ups must be part of a routine maintenance program for all electronic records.
- If a specific proprietary software application is being used, back-ups must include architecture as well as content.
- Back-ups should be stored in a location that is more than 15 miles from the source, and in a secure environment suitable for data media storage.

Note: A back-up is considered a duplicate record. It should not be retained longer than is necessary to ensure restoration after a disaster or crash. The copy of the record that resides on a back-up tape is subject to audit, litigation, and public records requests as long as the back-up exists. Therefore, it should never be retained longer than the retention period of the records it contains.

Minimum Security Standards

All University computers and computing devices must be properly managed and protected from intrusion and misuse by unauthorized entities. The following steps must be taken to ensure the security of the records in individual office as well as the computer networks at the UW:

- System access accounts for users must be based on a unique identifier (login).
- No shared account is allowed except as authorized by the system owner or operator and where appropriate accountability can be maintained.
- Users' system access should be based on the principle of least privilege and the principle of separation of duties.
- All vendor issued patches for software or operating systems must be applied in a timely manner to prevent the systems from being compromised and/or causing disruptions of network services and/or other systems.
- Externally accessible systems must install antivirus software and maintain procedures for regular signature updates.
- Vendor software and systems are required to have the capability to log basic information about user access activity, system changes, and events for the possible creation of historical logs and access violation reports. Logs must be monitored for intrusions or attempts at unauthorized access.
- Vendor software and systems must maintain a functioning and accurate system clock, since it is a critical element for the computer forensics and system logs that are essential for successful investigations in case of a breach of security.
- When an employee separates, their immediate manager is responsible for notifying all system owners and operators, or the designated system administrator handling the computer or communications accounts, to close all related accounts and remove all access capabilities related to the separated employee.
- A growing number of office machines, such as printers, copiers, and fax machines, are now network-connectable. These devices may retain copies of documents that have been scanned or copied on them. In most cases it is possible to configure these devices to automatically delete stored information. We highly recommend implementing automatic deletion, if practicable.
- If the documents to be scanned contain UW Confidential data, additional security controls might be necessary. Organizations should contact the UW Privacy Office for advice.
- Potential incidents of security breaches should immediately be reported:
    - Potential incidents involving national security information or national security systems must be reported only to the University Facility Security Officer.
    - Potential incidents involving protected health information must be reported to the appropriate jurisdiction, either UW Medicine Compliance or for clinics that are not part of UW Medicine, to the Executive Director of Health Sciences Administration.
    - Potential incidents unrelated to national security information, national security systems, or protected health information must be reported to the Office of the University Chief Information Security Officer (CISO) and the Privacy Office.

Implementing Destruction

It is extremely important to ensure that scanned records are not destroyed before the end of their retention period. The following strategies must be incorporated into scanning procedures to ensure records are deleted/purged in accordance with approved records retention schedules:

- Ability to delete files is restricted to authorized users only.
- Files are not deleted without first being subject to an approval process.
- Approval to delete files is restricted to authorized individual(s).

- All authorized deletions of scanned records (including by system administrators) are recorded in an audit log. This can include:
  - Document type
  - Original document date
  - Deleted by
  - Date deleted
  - Deletion authorized by

Process Documentation

Written documentation for the process used to scan records must be created by each office who takes responsibility for scanning a paper record that will result in the destruction of the original paper. The responsibility is based on the scanning process, rather than who will be responsible for maintaining the scanned image. **A copy of this written documentation (paper or electronic) must be filed with UW Records Management Services.**

Documentation will include:

- Instructions for the use of scanning hardware, including scanning settings.
- Instructions for quality control inspections.
- Suggestions for how scanned records are to be enhanced or manipulated in order to create a more readable image.
- Include, in detail, the steps that will be taken to correct a scanned record that is not clear and is difficult to read (not complete, blurry, or otherwise illegible).
- Standards and instructions for indexing, naming and filing scanned documents.
- Back-up procedures for the electronic repositories of all scanned records.
- The process used to identify images that have past their retention period.
- The process and individual(s) authorized to approve destruction of records.
- The process through which these images will be permanently deleted/purged.