UW SCANNING REQUIREMENTS

Scanning or Imaging is the process by which paper documents are copied and saved as digital images. These digital images or electronic records are saved as PDF or TIFF files. Scanning paper records does not automatically authorize the destruction of the source documents from which the scanned images have been created. However, if scanned following the requirements in this document, the electronic record can legally take the place of the paper document; which can then be destroyed.

Like all electronic records scanned files must be 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.

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 replacements for the original paper records.

The requirements begin with a consultation which must be scheduled with UW Records Management Services at the beginning of this process, before records are scanned.

1) RECORDS RETENTION

a) RETENTION OF SCANNED RECORDS

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.

Once paper records are scanned according to the technical requirements outlined in this document, the paper records can be destroyed. It is, however, important to note that the retention period which would have been applied to the paper record must instead be applied to the scanned record.

2) TECHNICAL SCANNING REQUIREMENTS

a) FORMATS AND SCANNING DENSITIES

Black and white, gray, and color paper records can be scanned. (Any kind of record can be scanned including color text documents, photographs, and maps, plans, and engineering drawings.)

- Scanners must be set at a minimum of 300dpi (dots per inch); and

- Scanned records must be saved as PDF or TIFF files.

  Note: JPEG is not acceptable if the scanning is done with the intention of destroying the original paper records.

b) QUALITY CONTROL

Scanned document images must be inspected visually to ensure they are complete (the entire document has been captured), clear and easily read.

It is Highly Recommended That:

- Each scanned record is 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); and

- The number of original paper documents must be compared to the number of scanned records to ensure that every document was scanned.

At a Minimum:

While it is highly recommended that each document is reviewed to ensure its completeness, clarity and usability, scanned documents can be reviewed in batches through a process called Sampling:

- Every 10th document is reviewed to ensure the scanning quality is consistent and the images are usable; and

- The number of original paper documents must be compared to the number of scanned records to ensure that every document was scanned.

c) 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.

- Sometimes 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.

- If 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 above 300 dpi and scan again. Keep increasing the dpi until the record is as readable as possible.

- Sometimes because of the condition of the original paper record, a good quality scanned image cannot be produced. In these cases it is necessary to document this 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".
        - When saving to an networked drive or storage location (e.g. I-drive) use Acrobat Pro "Additional Metadata" in the Document Properties description tab; or

    - When indexing/naming the document include, "best scan possible".

d) 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.

This documentation includes:

- Instructions for the use of scanning hardware, including scanning settings; and

- Standards and instructions for indexing, naming and labeling files; and

- Instructions for Quality Control inspections; and

- How scanned records are enhanced or manipulated 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 difficult to read (not complete, blurry, or otherwise illegible); and

- The process used to identify images that have past their retention period; and

- The process through which these images will be deleted/purged.

3) MANAGING SCANNED RECORDS

a) 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 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 large (size of the image and quantity of images) 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; and

- Save individual documents to folders. Include the year the records were either created or received in the folder title; and

- 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 on a regular basis.

If saving to a database:

- Configure the database or system so that records with the same retention are mapped; and
- 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

b) 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.

c) 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:

- Files are not deleted without first being subject to an approval process; and
- Approval to delete files is restricted to authorized individual(s); and
- Ability to delete files from an networked storage location (e.g. I-drive) is restricted to authorized users only; and
- Ability to delete files from a database is restricted to authorized users only; and
- 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

d) MIGRATION AND PRESERVATION STRATEGIES

Archival records and records with a retention period of more 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:

- 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; or
- 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; or

- 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

- When maintaining records with a records retention period of more than 6 years that are stored in a networked storage location (e.g. I-drive), files must be saved in the new operating system when a new version of windows is released; or

- 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. If files are stored in a system for which only proprietary extraction means are available or possible, then as soon as it is available, scanned records must be migrated to the format version supported by the most recent version of the software used to access and manage the files. New versions of the software cannot be skipped.

e) DISASTER PREPARADNESS 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; and

- If a specific software application is being used, back-ups must include architecture as well as content; and

- 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.

4) MINIMUM COMPUTER 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 (password), and no shared account is allowed except as authorized by the system owner or operator and where appropriate accountability can be maintained.

- Users' system access must 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. Always be sure to check the memory of your office machine and delete any copies of records that you find.

- If the documents to be scanned contain UW Confidential data, additional security controls might be necessary. Organizations should contact the Office for the CISO 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).