University Advancement
Scanning Requirements and Guidelines

Index

Overview

This scanning policy applies to all of University Advancement including staff in colleges, schools, units, and branch campuses. Some teams may have additional policies originating from their college, school, unit or campus. Where there are variances, school/college/unit-teams should default to their organization's policies. The procedures in this policy allow for a scanned image to legally replace the paper source document. Original paper copies of scanned documents can be destroyed as soon as the scanned image has been checked for quality control, saved, and backed-up in the appropriate electronic storage location. Scans will be retained for the entirety of their retention period as per the University General Records Retention Schedule and our departmental retention schedules. The requirements in this policy are based on Imaging Systems, Standards for Accuracy and Durability – Chapter 434-663 of the Washington Administrative Code (WAC). Any revisions made to this policy will need to be reviewed and approved by UW Records Management Services.

This document must be reviewed and approved by Records Management Services any time the policy is updated.

Scanning Requirements

- Scanners must be set at a minimum scan quality of 300 dpi (dots per inch).
- Scanned documents will be saved as PDF files for documents and as TIFF files for images.
- Scanned documents will not be modified from their original paper copy except to add notes and metadata when necessary.
- When scanning archival records, the University Archivist should be contacted to discuss ingestion of original paper documents.

UA also recommendations scanners should:

- have duplex capability (in order to automatically scan double-sided paper);
- have an automatic document feeder (to allow rapid scanning of multiple pages);
- be configured for OCR (to create searchable PDFs allowing for easier retrieval of documents);
- have auto-alignment and auto-rotation features enabled (to fix crooked and sideways scans).
    - If a unit uses a scanner without the auto-rotation function, they must use a software such as Adobe Acrobat to rotate the orientation of the scanned document so it appears upright on computer screens.

Quality Control Requirements

- Scanned documents will be visually inspected to ensure that the image is complete, clear, and readable.
    - For high volume scanning, every tenth document will be inspected.

- The number of pages in each scanned document must match the number of pages in each original paper document.
- If scanned images are crooked, incomplete, illegible, or otherwise compromised, the document will be rescanned until a readable scan is produced.
    - If a suitable scan is not produced, the original paper copy will be retained for the full retention period.

Image Enhancement

When a scanned document does not meet the Quality Control Requirements outlined above, one or more of the following actions should be taken to improve image quality:

- Clean the glass on the scanner.
- Place the document on the glass rather than using the document feeder.
- Increase the scanning resolution above 300 dpi (dots per inch).
- Scan in color rather than black & white.
- Adjust the scanner's darkness/contrast settings.
- Check if the scanner has a "background suppression" setting and that it is turned on.

Storage Location and Security

- Scanned records will be stored on the network shared drive (W: drive) either within your current department's groups folder under W:\groups\ua\ or within a network folder under W:\groups\workgrps\.
- When determining the best location for storage, consider the level of security your scanned documents require. If the scanned documents are confidential and should not be viewed by others within your unit, it is best to create a new folder under "workgrps" and restrict access to the minimum necessary. If the scanned documents can be shared and viewed by others within your unit, it is recommended scanned documents be saved to your current department folder under "ua".
- Colleges, schools, and departments that want to store scanned records outside of the W: drive should contact Records Management Services to create their own scanning policy using this policy as a template.
- The network shared drive is backed up daily by UW-IT.
- Access to electronic records will be restricted, at a minimum, by login and password. Shared accounts are permissible as authorized by the system owner/manager and where appropriate accountability can be maintained.
- If the electronic records contain confidential data requiring additional security controls, the Office of the CISO should be contacted for advice on the need for additional security.
- When an employee separates, their immediate manager is responsible for taking appropriate steps to ensure the access capabilities of the separated employee are revoked.
- All scanning devices will be configured to automatically delete stored information from memory or, failing that, will have their memory cache wiped prior to disposal of the unit.
- Potential information security and privacy incidents should immediately be reported to the appropriate individual(s) with delegated authority as defined in Administrative Policy Statement 2.5: Information Security and Privacy Incident Reporting and Management Policy.

Filing and Organization

Adhering to a consistent file storage convention will ensure that records can be found easily, and that timely and efficient destruction of scanned records that have met retention periods can occur. The folder structures below were designed so that units may delete entire folders of scanned records, instead of reviewing and deleting individual files.

Scanned records will be organized by topic and date as appropriate for the file type, examples of which are outlined in the following filing plan:

Donor Records

- Donor Files
  - [*Donor Name - Last, First*] [*AdvanceID#*]

Personnel/Employment Records

- Employee Files
  - [*Employee Name - Last, First*]
  - [*Employee Name - Last, First*] [*Year of Separation*]

Financial/Budget Records

- Financial
  - [*Type of Records*]
    - [*Fiscal Year/Biennium*]
      - [*Team*]

Reports, Meeting Agendas, and Notes

- [*Type of Records*]
  - [*Year*]
    - [*Report/Meeting/Committee Name*] [*Date - MM-DD-YYYY*]

Permits, Contracts, Projects, Events, etc.

- [*Type of Records*]
  - Current-Active
    - [*Permit/Contract/Project/Event Name*]
  - Past-Concluded
    - [*Year*]
      - [*Permit/Contract/Project/Event Name*]

When filing scanned records other than the ones listed above, use the retention period as a guide to determine how the records should be best organized for easy retrieval and destruction. Any filing system you create should include both an appropriate identifier and a time component based on the retention cutoff.

Destruction Process

- After scanning records and complying with quality control requirements, the original paper should be disposed of immediately.
- Like all electronic records, scanned records will be maintained in such a way as to ensure the records are accessible and readable for the entirety of their retention period.
- Destruction of scanned records requires a two-person review process.
- The Unit Managers, Administrative Assistants, and/or other appointed staff will perform an annual review at the end of the calendar year to identify records that have met their retention and are eligible for disposition.

- The unit's Executive Leadership Team member (or an appointed delegate) will review the compiled list of records that have met their retention and approve their disposition.
- Upon receiving approval, the initial reviewer will be responsible for deleting the records and completing the Disposition Log.
- Records that are responsive to ongoing or pending audits, lawsuits, or public disclosure proceedings will not be destroyed until the issue is resolved and our office is specifically advised that such records may be destroyed.
    - It is the responsibility of both the reviewer and Executive Leadership Team (ELT) member to properly identify any records that are on destruction hold during the review/approval process.

Useful Web Links

UW General Records Retention Schedule: https://finance.uw.edu/recmgt/gs/

UW Departmental Retention Schedule Search: https://finance.uw.edu/recmgt/depts/

Shredding Services: https://finance.uw.edu/recmgt/faq?tid=Shredding

Destruction Log: https://finance.uw.edu/recmgt/managing/pastretention#destruction-log

Approved by:

DocuSigned by:
Julie L. Brown
3C892B543CE6465...

6/4/2020
Date

Julie L. Brown
Associate Vice President / Chief Operating Officer & Chief Budget Officer
University Advancement

DocuSigned by:
Barbara Benson
B5252382465484...

6/4/2020
Date

Barbara Benson
Director
Records Management Services