

Office of Public Records & Open Public Meetings Scanning Policy

Purpose

This scanning policy applies to the Office of Public Records & Open Public Meetings. The procedures in this policy allow for a scanned image to legally replace the paper source document. Scans will be retained for the entirety of their retention period as per the [University General Records Retention Schedule](#) and our departmental retention schedule. Original paper copies of scanned documents will be disposed of as soon as the scanned image has been checked for quality control, saved, and backed-up in the appropriate electronic storage location. 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.

Records in Ariba: Any documents scanned into Ariba according to the scanning and quality control requirements outlined in this policy legally take place of the paper documents. Because Ariba becomes the official “system of record” and, as such, will be responsible for maintaining the records for their legally approved retention period, our office will not keep paper or scanned copies of anything submitted through Ariba. For more information, please refer to the [University Ariba scanning policy](#) on the Records Management Services website.

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.
- 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.

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.
 - Only when a suitable scan cannot be produced will the original paper copy 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 the Nebula-MWS network shared drive, Microsoft OneDrive, and the AccessPro database located on a UW server.
- Access is restricted to current employees of the Office of Public Records and Open Public Meetings.
 - Access to OneDrive of Personnel Files will be restricted to the Director and the two Officers.
- These locations are backed up daily by UW-IT and Microsoft.
- 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

Our office will organize scanned records according to the following filing plan:

Walk-In Public Records Requests and Potentially-Responsive Records Received from Departments

- These will be scanned onto the network shared drive then uploaded into the AccessPro database.
- Records are organized by PRR number.
- Original paper records will be destroyed immediately upon completion of a successful scan.
- Copies saved to the network drive will be kept for six months to allow sufficient time to ensure scans are properly ingested into AccessPro.
- The copy uploaded into AccessPro serves as the official copy and will be retained for the full retention period.

ProCard Transaction Detail Reports

- Signed copies of the ProCard Transaction Detail Reports will be scanned and sent to Finance.
- Original paper records will be destroyed immediately upon completion of a successful scan.
- No copies of the Transaction Detail Reports will be retained within the Office of Public Records & Open Public Meetings.

Personnel/Payroll/Training Records

- Current Staff
 - [Employee Name - Last, First]
- Separated Staff
 - [Year]
 - [Employee Name - Last, First]

Disposition Process

- Like all electronic records, scanned records will be maintained to ensure the records are accessible and readable for the entirety of their retention period.
- Staff will perform a quarterly review to identify records that have met their retention and are eligible for disposition.
 - Records will be identified for disposition based on the retention date included in the folder title.
- Two people will review the compiled list of records that have met their retention to ensure accurate disposition of records.
- Upon completion of the review, the Program Operations Specialist/Manager of Compliance and Legal Affairs will review the compiled list of records that have met their retention and approve their disposition.
- Upon approval, the Program Operations Specialist/Manager of Compliance and Legal Affairs 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 approver to properly identify any records that are on destruction hold during the review/approval process.