

Compliance and Risk Services: Claim Services Scanning Policy

This scanning policy applies to Claim Services. 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 schedule. The requirements in this policy are based on Imaging Systems, Standards for Accuracy and Durability – Chapter 434-663 of the Washington Administrative Code (WAC).

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.
 - 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 Access

- Scanned records will be stored Nebula-MWS network shared drive and the *Riskmaster* departmentally-managed database.
- Nebula-MWS is responsible for backup of information on the network shared drive.
- UW-IT is responsible for backing up the *Riskmaster* database.

- Access to all repositories is restricted to current employees of Compliance and Risk Services and authorized members of UW-IT.
- We affirm that our storage location meets all security and privacy requirements as outlined by the University of Washington Office of the Chief Information Security Officer.

Filing and Organization

Our office will organize records scanned to the Nebula-MWS network shared drive according to the following filing plans:

Potential Claims/Incident Reports/Accident Reports

- Claims
 - _Potential Cases
 - [Case type, ex. Auto Liability]
 - [2-digit year] Archived Potentials
 - [Potential case name, ex. last, first]
 - [Potential case name, ex. last, first]

General Claims Subject Files

- Claims
 - [Subject file, ex. Brief Bank]
 - [Sub-subject, ex. ADA & Faculty Issues] (where applicable)
 - [Document name] [4-digit year].pdf

Security Standards

All University computers and computing devices must be properly managed and protected from intrusion and misuse by unauthorized entities. The following steps will 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). Shared accounts are allowed when as authorized by the system owner or operator and where appropriate accountability can be maintained.
- 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 or, when that is not practicable, instituting a practice of manually clearing the device's memory.

- If the documents to be scanned contain confidential UW data, additional security controls might be necessary. Organizations should contact the Office of the University Chief Information Security Officer (CISO) for advice.
- Potential incidents of security breaches should immediately be reported to the Office of the CISO.

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.
- The Director 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.
 - Records stored on the network shared drive for Claim Services will be identified for disposition based on information in the file/folder names.
 - Records in *Riskmaster* will be identified for disposition using a database query.
- The Director will review the compiled list of records that have met their retention and approve their disposition.
- Upon approval, the Director or their designee 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 the Director of Claims Services to properly identify any records that are on destruction hold during the review/approval process.