W **SCHOOL OF DENTISTRY**
UNIVERSITY *of* WASHINGTON

SCANNING AND STORING ELECTRONIC RECORDS POLICY

UW Scanning Requirements will be followed by the School of Dentistry.

Effective November 9, 2018 the School of Dentistry is no longer required to save paper copies of financial documents. Electronic scanned copies of the paper documents will replace them. This change requires that departments produce properly scanned documents. Once paper records are scanned according to the requirements outlined in this document, the paper records can be destroyed.

- **Exception:** When it is not possible to create a readable scanned image, the original paper document must be kept and UW records retention policies must be adhered to.

It is important to note that the retention period which would have been applied to the paper record must instead be applied to the scanned record.

All 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 website.

Records Applicable for Electronic Scanning
- Invoices
- Packing slips
- ProCard receipts
- Signed approval forms/email approvals
- Signed ProCard accounting notes and detail
- Credit card receipts for students' purchases of supplies outside of regular dental issue items
- Contracts and Agreements
- Business Associate Agreements (BAA)
- Data Security Agreements (DSA)

Scanner Settings
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 300 dpi (dots per inch)
- Scanned documents will be saved as PDF files
- Scanned documents will not be modified from their original paper copy

Quality Control
School of Dentistry employees must visually inspect their scanned documents to ensure they are complete, clear and easily read:

- Scanned records must be compared to the original paper document to ensure accuracy
- The number of pages in each scanned document must match the number of pages in each original paper document.

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. These common problems must be corrected and addressed prior to departmental acceptance as a scanned image:

- Speckles or spots on the scanned image
- Skewed images that are not properly aligned
- When only part of the document is captured by the scanner
- When the scanned record is of poor quality and is not clearly readable
- See http://f2.washington.edu/fm/recmgt/scanning "Image Enhancement" for more information

Storage and Backup Policy

Files containing scanned documents subject to the retention requirements of this policy will be stored only on approved network storage, which is located on the "\\sod\files (S:)" drive. Network storage containing these scanned documents will be included in the department's backup schedule for business-critical data. Data from the School of Dentistry servers is backed up every business day by UW-IT and stored at the data center in Spokane.

Record Filing and Identification

The following organization will be applied to scanned documents:

Financial/Budget Records will be saved in S:\Finance first by org code, then by fiscal year, then by budget number, then by month.

📁 S:

    📁 Finance

        📁 [*Org Code*]

            📁 [*Fiscal Year/Biennium]*

                📁 [*Budget #*]

                    📁 [*Month*]

- Each scanned document must include the following information somewhere in the file name, but in no particular order: vendor name, date of invoice, and dollar amount.
- Additional information such as the object code or transaction number may be included as well, but is not required.
- Access to the S:\Finance folders is limited to:
    - An "Administrative group" composed of key fiscal people within the SOD (i.e. Assistant Dean of Finance and Resources, Purchasing and Accounts Payable Manager, Purchasing team members, Clinic Accounting Director, etc.) who have access to all of the folders and files within the S:\Finance folder.

- o Individuals within each department (i.e. the department Administrator, department fiscal specialist, etc.) who have restricted access to only the org code folders which are related to their office.
- The Purchasing and Accounts Payable Manager will perform an annual audit to identify records that have reached the end of their retention period using the month/year information included in the folder names.
    - o Following their initial review, the Purchasing and Accounts Payable Manager will email each Department Administrator to approve the deletion of the files under the org code(s) they are responsible for.
    - o Upon receiving approval, file deletion will be conducted by the Purchasing and Accounts Payable Manager or his/her designated staff member.
    - o Approval of deletion and date of deletion must be documented in a disposition log.
    - o 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.
    - o 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.

Contracts and Agreements will be saved in S:\ Purchasing and Accounts Payable, separated into BAAs and DSAs and all other types of contracts. Each folder will be further divided into Active and Concluded subfolders. Expired agreements will be moved from Active to Concluded and filed by year of completion.

📁 S:

📁 Purchasing and Accounts Payable

📁 BAAs and DSAs

📁 Active

📁 Concluded

📁 [*Calendar Year*]

📁 Contracts

📁 Active

📁 Concluded

📁 [*Calendar Year*]

- Each scanned document must include the name of the contracted organization in the file name.
- Access to the S:\ Purchasing and Accounts Payable folders is limited to:
    - o An "Administrative group" composed of key fiscal people within the SOD (i.e. Assistant Dean of Finance and Resources, Purchasing and Accounts Payable Manager, Purchasing team members, Clinic Accounting Director, etc.) who have access to all of the folders and files within the S:\Purchasing and Accounts Payable folder.
- The Purchasing and Accounts Payable Manager will perform an annual audit to identify any contracts/agreements that have expired since the last review.
    - o Expired contracts/agreements will be moved into the Concluded folder and filed by the calendar year in which they were concluded.

- The Purchasing and Accounts Payable Manager will also perform an annual audit to identify expired contracts/agreements that have reached the end of their retention period using the year information included in the folder names.
    - Following their initial review, the Purchasing and Accounts Payable Manager will email the Assistant Dean for Finance and Administration (or his/her delegate) to approve the deletion of the files past retention.
    - Upon receiving approval, file deletion will be conducted by the Purchasing and Accounts Payable Manager or his/her designated staff member.
    - Approval of deletion and date of deletion must be documented in a 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.

Data 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 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 closing all related accounts and removing all access capabilities related to the separated employee. This includes access to Ariba applications through Astra, which is managed centrally in the School of Dentistry Dean's Office.
- If the documents to be scanned contain confidential UW data, additional security controls might be necessary. The School of Dentistry will remove sensitive information prior to attaching a document in Ariba. Such information could include credit card account information, home addresses, patient names etc.
- Potential incidents of security breaches should immediately be reported.

Approved: 11/14/2018