

**UNIVERSITY OF HOUSTON SYSTEM  
ADMINISTRATIVE MEMORANDUM**

**SECTION: Fiscal Affairs**

**NUMBER: 03.H.01**

**AREA: Records Management**

**SUBJECT: Records Retention**

---

1. PURPOSE

The purpose of this document is to establish principles and policies necessary to preserve the state records of the component university and to implement a system to store, access, and destroy these records in accordance with state guidelines.

2. POLICY

2.1. The Texas Government Code, Chapter 441, Section 441.183 requires state agencies to establish and maintain a records management program on a continuing and active basis.

2.2. The Texas Administrative Code (TAC), Title 13, Part 1, Chapter 6 provides specific requirements for maintaining a records management program. Each agency is required by Texas Government Code Section 441.185 to maintain a records retention schedule for state records and to submit this schedule to the state records administrator. This schedule must list the state records created and received by the agency, propose a period of time each record shall be maintained by the agency, and provide other information necessary for the operation of an effective records management program. .

2.3. The University of Houston System Records Retention Schedule has been prepared and filed with the state records administrator as required, and serves as the schedule for the System and each of the component universities. State regulations (13 TAC §6.3) require that the retention schedule be reviewed, updated, and re-certified annually for the first two years after the initial approval of the schedule and every three years thereafter. The System Records Retention Officer will coordinate changes recommended by the various components prior to final approval submission. All divisions/departments of the system are required to adhere to the retention guideline and schedule noted above prior to storing state records or requesting destruction of the records. Divisions/departments having custody of official state records must obtain approval for the destruction of those items from the designated administrative officer.

2.4. Section 441.184 of the Government Code states that each agency shall have a records administrator, appointed by the head of the agency, to ensure compliance with state law with reference to the preservation of state records.

3. Document Imaging Requirements for Financial Transactions

3.1. Scanned images and electronic files used as backup documents for financial transactions must meet the following requirements:

- a. Minimum scanning resolution of 300 dpi X 300 dpi (dots per inch), black and white.
- b. File type of TIF, PDF, RTF, TXT, Word, or Excel.
- c. All information necessary for transaction approval must be legible on the scanned image or electronic file.

3.2. Review of scanned images.

- a. The person who scans the image will verify that the image is legible before it is uploaded to the Finance system to avoid uploading inadequate images.
- b. The person who uploads the scanned image will verify it can be opened and is legible after it is uploaded as well.
- c. The final approver of the transaction will also verify that the uploaded image is acceptable. If not acceptable, the image will be made "Inactive" and the transaction initiator will be required to rescan and upload the backup document.

4. Financial Documents with Security Sensitive Information

4.1. The following information is considered security sensitive, and should not be included on documents uploaded to the Finance system unless otherwise noted in 4.3 below:

- a. Social security numbers;
- b. Bank account numbers;
- c. Credit card numbers; and
- d. Intellectual property or research data that could be considered proprietary, though this information is normally not included as backup to financial transactions.

4.2. Security sensitive information should be hidden on all documents uploaded to the Finance system (except those noted in 4.3) in one of the following ways:

- a. Make a copy of the document to be scanned, mark through the security sensitive information on the copy so it cannot be read, and scan the copy.
  - b. Scan the original document and mark the scanned image on the computer using the tools available in TIF (or Adobe Acrobat Writer for a PDF) before uploading the image to the Finance system.
  - c. If the original document will not be preserved, mark through the security sensitive information on the original document before it is scanned.
- 4.3. Security sensitive information should not be hidden on the following documents:
- a. IRS forms and tax-related documents with social security numbers required as backup to financial transactions should be uploaded with all information shown. When the document is reviewed for approval, Finance will designate the documents as “security sensitive” to hide them from view.
  - b. Vendor setup forms with social security numbers or bank information should be faxed to the UH Accounts Payable vendor maintenance group directly, but should not be included in voucher backup. Vendor setup forms will be hidden from most people because they are stored on vendor pages where a limited number of people have access.
- 4.4. Access to view “security sensitive” documents will only be granted to individuals in Finance who must review and approve the associated transaction, internal and external auditors, and others with a need to view this information, as determined by the component chief financial officer or designee.
5. Retention Requirements for Original Documents Uploaded to the Finance System
- 5.1. All original documents and files that are scanned and uploaded to the Finance system (i.e., hard copies of original documents) may be discarded after the associated financial transaction has completed has posted or completed its final approval, whichever is later, except in the following circumstances:
- a. Documents for transactions that are pre-approved for payment and reviewed for adequate documentation afterwards (e.g., local fund travel reimbursements at UH) should be maintained in the department’s files at least one week after payment is issued to allow adequate time for review.
  - b. Original IRS or other government documents that must be mailed or maintained in their original form.

5.2. Documents that cannot be uploaded to the Finance system because they exceed the maximum file size (60 MB) must be maintained in the files of the originating department for the period indicated in the records retention schedule.

6. REVIEW AND RESPONSIBILITIES

Responsible Party: Associate Vice Chancellor for Finance

Review: Every three years on or before April 1

7. APPROVAL

Approved: John Rudley  
Vice Chancellor for Administration and Finance

Jay Gogue  
Chancellor

Effective Date: November 30, 2005

8. INDEXING TERMS

Records  
Retention  
Scanning