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 universities, and

- comply with state and federal law,
- apply best practices for electronic and hard copy document retention and management,
- demonstrate fiscal responsibility and efficiency by eliminating the need for unnecessary extra file space (both computer file storage space and file cabinets/rooms), and
- define a system to store, access, and dispose of these records in accordance with state and federal 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's 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 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 five years thereafter. The System Records Retention Officer will coordinate changes recommended by the various universities 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, transferring records to the appropriate archivists, 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 Texas 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.

2.5. Each university shall designate an individual to serve as the liaison with the System Records Retention Officer to ensure university compliance with State Records Retention Requirements.

2.6. This policy relates to both hard copy and electronic records equally, including e-mail.

3. DOCUMENT IMAGING REQUIREMENTS FOR ALL UNIVERSITY BUSINESS TRANSACTIONS

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

3.1.1. Minimum scanning resolution of 300 dpi X 300 dpi (dots per inch), black and white.

3.1.2. File type of TIF, PDF, RTF, TXT, Word, or Excel.

3.1.3. All information necessary for transaction approval must be legible on the scanned image or electronic file.

3.2. Review of scanned images.

3.2.1. The person who scans the image will verify that the image is legible before it is uploaded to PeopleSoft or other institutional system to avoid uploading inadequate images.

3.2.2. The person who uploads the scanned image will verify it can be opened and is legible after it is uploaded as well.

3.2.3. 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. UNIVERSITY BUSINESS DOCUMENTS WITH SECURITY SENSITIVE INFORMATION

4.1. The following information is considered security sensitive, and should not be included on documents uploaded to PeopleSoft or other institutional system unless otherwise noted in Section 4.3 below:

4.1.1. Social security numbers;

4.1.2. Bank account numbers;

4.1.3. Credit card numbers; and

4.1.4. 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 PeopleSoft or other institutional system (except those noted in Section 4.3.) in one of the following ways:

4.2.1. 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.

4.2.2. 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 PeopleSoft or other institutional system.

4.2.3. 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:

4.3.1. IRS forms and tax-related documents with social security numbers required as backup to university business 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.

4.3.2. Vendor setup applications including social security numbers and bank information are submitted by vendors through the secured vendor management system. Once applications are processed and approved, security sensitive vendor information should be stored only in the vendor

file where the access is limited to the UH Accounts Payable vendor maintenance group.

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 university's chief financial officer or designee.

5. RETENTION REQUIREMENTS FOR ORIGINAL DOCUMENTS UPLOADED TO PEOPLESOFT OR OTHER INSTITUTIONAL SYSTEM

5.1. All original documents and files that are scanned and uploaded to PeopleSoft or other institutional system (i.e., hard copies of original documents) may be discarded after the associated financial transaction has posted or completed its final approval, whichever is later, except in the following circumstances:

5.1.1. Documents for transactions that are pre-approved for payment and reviewed for adequate documentation afterwards should be maintained in the department's files at least one week after payment is issued to allow adequate time for review.

5.1.2. Original IRS or other government documents that must be mailed or maintained in their original form.

5.2. Documents that cannot be uploaded to PeopleSoft or other institutional 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 University of Houston System's Records Retention Schedule.

6. CORRESPONDENCE

Correspondence shall be categorized into one of the following four categories as defined below: Administrative Correspondence, General Correspondence, Directives and Transitory Correspondence. This categorization is independent of media form and applies equally to electronic and paper records.

6.1. Administrative Correspondence is defined as incoming/outgoing and internal correspondence ,in any media, pertaining to the formulation, planning, implementation, interpretation, modification, or redefinition of the programs, services, or projects of the system and/or a university, as well as the administrative regulations, policies, and procedures that govern them. Administrative correspondence must be retained for 4 years.

For further information, see the University of Houston System's Records Retention Schedule.

6.2. General Correspondence is defined as any non-administrative incoming/outgoing and internal correspondence, pertaining to or arising from the routine operations of the policies, programs, services, or projects of the System and/or a university. General correspondence must be retained for 2 years.

For further information, see the University of Houston System's Records Retention Schedule.

6.3. A Directive is defined as any document that officially initiates, rescinds, or amends university or general office procedures. Directives must be retained for 1 year past the date they are superseded.

For further information, see University of Houston System's Records Retention Schedule.

6.4. Transitory information is defined as records of temporary usefulness that are not an integral part of a record series, and that are required only for a limited period of time for the completion of an action. Examples include routine messages, telephone message notifications, internal meeting notices; routing slips, incoming letters or memoranda that add nothing of substance to enclosures; similar routine information used for communication, but not for the documentation, of a specific university transaction; an inquiry about department course offerings or scheduling issues, announcements, etc. Transitory records do not need to be retained beyond the time of their usefulness.

For further information, see the University of Houston System's Records Retention Schedule.

7. ROLES AND RESPONSIBILITIES

7.1. All university employees are expected to:

1. Appropriately identify and retain such records in accordance with this policy and the University of Houston System's Records Retention Schedule.

2. Regularly check for new messages or correspondences.

3. Routinely secure documents, records, and correspondences that are System/university/business records in accordance with the University of Houston System's Records Retention Schedule.

4. Delete transitory correspondence as soon as its usefulness has ended.

5. Retain a University/Business Record in accordance with Section 9.5 if the user is:

a. The sender or creator;

b. The only or main recipient; or

c. The designated university custodian for that type of information.

6. Retain documents, records, or correspondences only as long as required per the University of Houston System's Records Retention Schedule.

7.2. University information technology (IT) departments and all colleges/divisions/department will:

1. Establish and publish standards for e-mail account administration, storage allocations, and automatic archiving of messages to users' local computer folders files;

2. Provide active e-mail server facilities in compliance with this policy for all university business;

3. Provide the required end user training and help desk support for e-mail services;

4. Manage server implementations of legal holds that are issued by General Counsel; and

5. Suspend any automatic deletion processes that may be in place, as necessary, to preserve specific electronic messages, records and information that fall within the scope of the legal hold, and that reside on active e-mail servers.

7.3. Department heads and unit managers are responsible for notifying and providing message and records retention guidance to staff and faculty within their respective units. The guidance provided must be in accordance with this policy and the University of Houston System's Records Retention Schedule.

7.4. The System records retention officer appointed by the Chancellor is responsible for providing guidance to System personnel in ensuring compliance with state law with reference to the preservation of state records. Each university has a records retention liaison to ensure compliance.

7.5. System/university employees who have been notified by General Counsel of a legal hold are responsible for preserving all messages, records, and information that fall within the scope of the hold that they have downloaded and/or stored locally. For more information on legal holds please see Section 10.

8. CLASSIFICATION OF DOCUMENTS, RECORDS AND CORRESPONDENCES

8.1. Questions about the proper classification pursuant to the University of Houston System's Records Retention Schedule of a specific message, record, document or piece of information should be directed to the employee's manager or business administrator. If further assistance is needed in classifying information, the System Records Retention Officer should be contacted for assistance.

8.2. The burden of determining whether a specific message is a System/university/business record should fall to the department responsible for being custodian of those records. For example, Human Resources are responsible for determining whether messages sent to Human Resources pertaining to employee relations are classified as university records.

9. E-MAIL RETENTION

9.1. Non-Business Use of E-Mail or Electronic Media Services

The computers, electronic media and e-mail messaging services provided by the System or its universities are primarily for business use. Incidental personal use of a University Account Mailbox is allowed according to the Acceptable Use Policies of each university. Personal, non-business related e-mail or electronic media messages are not university records and do not need to be retained.

9.2. Transitory E-mail

A. Most e-mail messages are created primarily for routine communication or information exchange that is of temporary usefulness which is not an integral part of the System or university's recordkeeping system, i.e., they are not university records. These messages should be considered transitory correspondence that do not have lasting value and should be:

1. Read and deleted; or

2. Read and retained on the active mail server for no longer than necessary or until their usefulness has ended (whichever occurs first), and then deleted; or

3. Read and retained on the active mail server or moved to other file locations when job requirements necessitate retention, and then deleted when their usefulness has ended.

9.3. System/University/Business Records

When the contents of an e-mail message exhibit one or more of the following characteristics, it should be classified as a system/university/business record:

A. Has operational value (required by a department to perform its primary

function)

1. Administrative actions taken or planned

2. Reports or recommendations

3. Policies, procedures, guidelines, rubrics, or templates

4. Non-transitory communication pertaining to routine operation of policies, programs services or projects of the university or of a department

B. Has legal or evidential value (required to be kept by law), such as a legal hold or investigation (see Section 8.1 below).

C. Has fiscal value (related to the financial transactions of the campus), required for financial reporting and audits.

D. Has historical significance (of long-term value to document past events). These messages may arise from exceptional age and/or some significant historical event.

E. Has vital value (critical to maintain to ensure operational continuity after a disruption or disaster). Vital records or information may fall into any one of the above value categories.

9.4. To assist in the determination of whether an e-mail is a System, university or business record or is transitory in nature, see http://www.uh.edu/emailretention.

9.5. E-mail messages that are System/university/business records should:

A. Be moved to dedicated storage on a university approved location (i.e., department file share, cloud storage); or

B. Be retained on the university e-mail server.

C. Messages should be stored in a manner that can be retrieved easily by the university.

9.6 Backup Files

Backup images of university e-mail servers hosted on-site should be kept for no more than twelve (12) weeks. These backup images are for system restoration and disaster recovery purposes, and are not designed to facilitate retrieval of deleted messages.

10. LEGAL HOLDS

10.1. When litigation against the System or its employees is filed or threatened, the law imposes a duty upon the System to preserve all documents and records that pertain to the issues. When the System Office of General Counsel is made aware of pending or threatened litigation, a legal hold directive will be issued to the legal custodians.

A legal hold directive overrides this records retention policy, as well as any records retention schedules that may have otherwise called for the transfer, disposal or destruction of relevant documents, until the hold has been cleared by System Office of General Counsel.

E-mail and accounts of separated employees that have been placed on legal hold status by the Office of General Counsel will be maintained by UHS Information Security until the hold is released.

No employee who has been notified by System Office of General Counsel of a legal hold may alter or delete or destroy any records that fall within the scope of that hold. An employee notified by System Office of General Counsel of a legal hold will be required to provide copies of the referenced documents or electronic records that the employee has downloaded and saved or moved to some other storage account or device.

10.2. In the event of litigation, the System chief information security officer will be the designated 30(b)(6) witness as defined by the Federal Rules of Civil Procedure.

10.3. When an open records request (or Public Information Act request, also known as a Freedom of Information Act Request) is pending, documents must be maintained while the request is pending.

11. REVIEW AND RESPONSIBILITY

Responsible Party: Associate Vice Chancellor for Finance

Review: Every five years

12. APPROVAL

Approved: */Raymond Bartlett/*
Senior Vice Chancellor for Administration and Finance

/Renu Khator/
Chancellor

Date: September 22, 2021