

*No certification necessary. Not considered policy, but a minor clarification of policy language. 9/13/10*

**UCC 0165 10F**

**Page 1 of 5**

**UNIVERSITY of HOUSTON**

**MANUAL OF ADMINISTRATIVE POLICIES AND PROCEDURES**

RECEIVED AUG 30 2010

**SECTION:** Information Technology  
**AREA:** User Guidelines

**Number:** 10.03.07

**SUBJECT:** Email Retention and Discovery

**I. PURPOSE AND SCOPE**

This policy is adopted in order to comply with state and federal law, to preserve emails which are state records of the university, to demonstrate fiscal responsibility by eliminating the need for unnecessary computer file storage space, and to apply best practices for electronic records retention at the university. This policy applies to 1) All email systems provided or funded (in part or in whole) by the University of Houston; 2) All users and account holders of university email accounts; and 3) All email messages sent or received using university email systems.

**II. POLICY**

**A. Non-Business Use of E-Mail Services**

The computers, electronic media and email messaging services provided by the university are primarily for business use. Limited, occasional or incidental use of electronic media (sending or receiving) for personal, non-business purposes is acceptable, provided that such use is done in a manner that does not negatively affect the systems' use for their business purposes. Personal, non-business related email messages are not university records and do not need to be retained.

**B. Transitory Correspondence**

1. Most email messages are created primarily for routine communication or information exchange that is of temporary usefulness which is not an integral part of the 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:

- a. Read and deleted; or
- b. 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
- c. 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.

2. Transitory correspondence is not essential to the fulfillment of the statutory obligations or to the documentation of university functions. Examples of transitory correspondence are:

- a. Routine messages

## Email Retention and Discovery

MAPP 10.03.07

- b. Telephone message notifications
- c. Notices about internal meetings or events
- d. Routing slips
- e. Incoming letters or memoranda of transmittal that add nothing of substance to enclosures
- f. Similar routine information used for communication but not for the documentation, of a specific transaction
- g. An inquiry about department course offerings or scheduling issues
- h. Announcements, etc.

## C. University/Business Records

1. When the contents of an email message exhibit one or more of the following characteristics, it should be classified as a university/business record:
  - a. Has operational value (required by a department to perform its primary function)
    - i. Administrative actions taken or planned
    - ii. Reports or recommendations
    - iii. Policies, procedures, guidelines, rubrics, or templates
    - iv. 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 "Legal Holds" 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). 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.
2. University/Business records, including messages and information, must be retained as noted in SAM 03.H.01 – Records Retention (<http://www.uh.edu/sam/3FiscalAffairs/3H1.pdf>) and in accordance with the Texas State Records Management Statutes. See in particular, Section 1.1 on General Administrative Records.

## Email Retention and Discovery

MAPP 10.03.07

3. To assist in the determination of whether an email is a university or business record or is transitory in nature, see <http://www.uh.edu/af/survival/IT/email-retention.pdf>.

4. Email messages that are university/business records should:

- a. Be moved to dedicated storage on departmental/office networked file systems (the equivalent of an electronic filing cabinet); or

Be retained on the active e-mail server. The active e-mail server is a computer on the university network that provides "post office" facilities for current users. It receives and stores incoming mail for users and forwards outgoing email for delivery. Users are assigned individual "mailboxes" where incoming and outgoing email messages are stored until deleted by the user.

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

D. Responsibility for Retention of Messages that are University/Business Records

The burden of determining whether a specific message is a university/business record should fall to the department responsible for being custodian of those records. For example, Human Resources is responsible for determining whether messages sent to Human Resources pertaining to employee relations are classified as university records. Other recipients should not retain messages longer than required for their respective job purposes. When that need no longer exists, the message should be deleted. In other words, only the department responsible for retention of a specific type of information or record is responsible for retention and disposition of its counterpart in electronic form.

Questions about the proper classification (transitory correspondence or university/business record) of a specific message, record, or piece of information should be directed to the employee's manager or college/division business administrator. If further assistance is needed in classifying information, the System Records Retention Officer should be contacted for assistance.

All university email users are expected to:

1. Regularly check for new messages;
2. Routinely secure messages that are university/business records in accordance with Section C; and to
3. Delete transitory correspondence as soon as its usefulness has ended.

E. Backup Files

All university e-mail server administrators shall keep backup images of university email servers for no more than 12 weeks. These backup images are for system restoration and disaster recovery purposes, and are not designed to facilitate retrieval of deleted messages.

F. Legal Holds

## Email Retention and Discovery

MAPP 10.03.07

1. When litigation against the university or its employees is filed or threatened, the law imposes a duty upon the university to preserve all documents and records that pertain to the issues. When 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 email 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 General Counsel.

Email and accounts of separated employees that have been placed on legal hold status by General Counsel will be maintained by Information Technology until the hold is released.

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

2. 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.

### III. ROLES & RESPONSIBILITIES

- A. Information Technology (IT) and all colleges/divisions/departments who provide independent mail services will:
  1. Establish and publish standards for email account administration, storage allocations, and automatic archiving of messages to users' local computer folders/files;
  2. Provide active mail server facilities in compliance with this policy for all university business;
  3. Provide the required end user training and helpdesk support;
  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 mail servers.
- B. 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 Texas State Records Retention Schedule.
- C. The university records retention officer appointed by the President is responsible for providing guidance to university personnel in ensuring compliance with state law with reference to the preservation of state records.

## Email Retention and Discovery

MAPP 10.03.07

- D. Originators and custodians of electronic messages, records, and information that are university/business records are responsible for:
1. Appropriately identifying and retaining such records in accordance with this policy and the Texas State Records Retention Schedule; and,
  2. Seeking assistance from their respective managers or college/division business administrators when unsure about how to categorize specific types of messages.
- E. 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.
- F. In the event of litigation, the chief information security officer will be the designated 30(b)(6) witness as defined by the Federal Rules of Civil Procedure.

## IV. RELATED INFORMATION

- A. For information about the Federal Rules of Civil Procedure, visit [http://www.uscourts.gov/rules/EDiscovery\\_w\\_Notes.pdf](http://www.uscourts.gov/rules/EDiscovery_w_Notes.pdf).
- B. For information about the Texas State Library Records Retention Policy, visit <http://www.tsl.state.tx.us/slr/recordspubs/stbull01.html>.
- C. For information about the System Record Retention Policy, visit <http://www.uh.edu/sam/3FicsalAffairs/3H1.pdf>.

## V. REVIEW AND RESPONSIBILITY

Responsible Party: Associate Vice President for Information Technology

Review: Every two years, on or before September 1

## VI. APPROVAL

---

Executive Vice President for Administration and Finance

---

President

Date of President's Approval: \_\_\_\_\_