UNIVERSITY OF HOUSTON SYSTEM
ADMINISTRATIVE MEMORANDUM

SECTION: Information Technology **NUMBER: 07.A.07**

AREA: Computing Services

SUBJECT: Use of Electronic Messaging Services by Employees

1. PURPOSE

The purpose of this policy is to define the appropriate use of and employee access to University of Houston System (UHS) electronic messaging services by faculty and staff employees.

2. POLICY STATEMENT

It is the policy of the University of Houston System to ensure employees use university assigned messaging services to conduct official System business, as opposed to personal e-mail accounts or non-university services.

3. DEFINITIONS

3.1.1. E-mail Alias – An e-mail address that serves as a pointer that directs e-mail messages to a destination e-mail account mailbox.

3.1.2. Electronic Messaging – Communications that include e-mail, unified messaging, voicemail and Instant Messages (IM).

3.1.3. University Enterprise Messaging Services – Electronic messaging and other applications provided as a service by the component university central IT department for campus-wide use.

3.1.4 University Account Mailbox – An account on a university mail/messaging server where electronic messages are delivered. This includes mailboxes managed by component university central IT departments, as well as those managed by individual campus departments.

4. POLICY

4.1.1. Use of University Enterprise Messaging Services

Each UHS component university provides enterprise communication services for use by employees conducting university business.

A. Employees are required to use University Enterprise Messaging Services for official business.

B. Non-University Enterprise Messaging Services should only be used for university business when that particular service is not provided by the component university's central IT department.

4.1.2. Current UHS Employees

A. All employees will be issued an E-mail Alias and/or a University Account Mailbox upon hire. Accounts will be created based on the information contained in the Electronic Personnel Action Request (ePAR) processed by Human Resources. Employees are required to use their issued E-mail Alias and University Account Mailbox for all official university business representing themselves as an employee. In the event of a UHS or component university-declared emergency, exceptions may be made to this policy by the UHS Chief Information Officer (CIO) or component university CIO in consultation with the component university HR officer.

B. The destination address for a current employee's e-mail alias must be a University Account Mailbox.

C. Employees may access their University Account Mailbox using smartphones, tablets or other portable devices and create forwarding rules on their University Account Mailbox allowing for copies of messages to also be sent to other non-university mailboxes. However, it is the employee's responsibility to ensure compliance with all university policies regarding data protection and confidentiality. Personal devices used for accessing University Account Mailboxes should be protected by a password or equivalent security and should support remote wipe or removal of e-mail in the event of device loss or theft. Employees should work with their campus IT staff in the event that their device is lost, stolen or compromised to assist in protection of university data.

D. Employees are responsible for ensuring that electronic messages that are university business records are maintained on university information resources in accordance with all appropriate record retention requirements as defined in SAM 03.H.01, Records Retention.

4.1.3. Current Employees on Leave

A. Employees are responsible for working with their supervisor prior to their departure to ensure business continuity concerns will be addressed during their absence. This could include configuration of an out of office/auto response message or establishing appropriate mail forwarding rules.

B. If the employee is not available and a business need exists that requires configuration of out of office/auto response messages or incoming message forwarding, approval must be obtained by contacting the component campus Information Security Officer, who will review the matter in consultation with the component campus Human Resource Officer and UHS General Counsel before authorizing.

4.1.4. Employees Separating from the University of Houston System or a UHS Component University

A. Employees may not retain their E-mail Alias upon leaving the university.

B. Employees will have their University Account Mailbox access removed according to the account termination date as defined on the ePAR. Continuing temporary employees or employees with no terminating ePAR (i.e., adjunct faculty) may have their account access bridged between multiple assignments. Account access must be removed after their last/terminal assignment.

1) Removal of Personal Messages – Employees are responsible for removing all personal messages from their University Account Mailbox prior to their last date of employment. It is the employee’s responsibility to notify any personal contacts of their new contact information.

2) Removal of University-related Messages from Personal Devices and Non-University Accounts – Employees are responsible for removing all messages considered university business records from any personal accounts where they may have been forwarded, as well as from their personal devices, such as smart phones, prior to their last date of employment.

C. Business Continuity

1) University departments are encouraged to utilize general department contact information (phone numbers, e-mail aliases, etc.) rather than employee-specific contact information for official business uses when possible. This provides the opportunity for electronic communications to continue to be routed to appropriate staff without needing to notify customers of changes in personnel.

2) Out of Office/Auto Response Messages – Prior to leaving the university, employees are responsible for setting an approved Out of Office/Auto Response message on their accounts (e-mail, voicemail, etc.) with appropriate university contact information.

Out of Office/Auto Response Messages will be in effect for 30 days after termination unless other arrangements are made with the UHS component IT department. After 30 days, all messages sent to the account will be rejected.

3) Forwarding of Incoming Messages – Generally, incoming messages received after an employee's departure from the university should not be forwarded from a former employee's account to a supervisor or other employee. In the event that a business need exists that requires incoming message forwarding, approval must be obtained by contacting the UHS component university Information Security Officer, who will review the matter in consultation with the UHS component university Human Resource Officer and UHS General Counsel before authorizing.

4) Updated Contact E-mail Address – Prior to their last day of employment, employees are responsible for updating PASS with a current personal e-mail address to ensure continued receipt of communication from Human Resources.

In the event there is a university need for the employee to maintain use of their University Account Mailbox or E-mail Alias after separating from the university, through termination, retirement, etc., the request must be made by completing the PeopleSoft Person of Interest (POI) process/sponsored account process through their department. The sponsored account form should be approved by the UHS component university Human Resources department and submitted to the component university IT department.

D. Acceptable Use and Expectation of Privacy

1) University Account Mailboxes are provided to faculty and staff for official university business in support of the mission and goals of the university. Incidental personal use of a University Account Mailbox is allowed according to the Acceptable Use Policies of each UHS component university.

2) All messages, files, and documents, including personal messages, files, and documents, located on university information resources are owned by the university, may be subject to open records requests, and may be accessed by the university in accordance with this policy. University employees, including supervisors, are not authorized to access the electronic messages of a current or former employee without their consent unless there is a business justification. Prior approval must be obtained by contacting the

UHS component university Information Security Officer, who will review the matter in consultation with the UHS component university Human Resource Officer and the UHS General Counsel before authorizing access to the messages.

i. Users of university information resources have no expectation of privacy while using a university information resource except as otherwise provided by applicable privacy laws. Access to user electronic messages may only be granted in accordance with Section IV.D.2 above.

ii. Use of electronic messaging must be in compliance with applicable laws and regulations. Users should be aware that the university may filter, block, and/or remove potentially harmful code from electronic messages. The use of electronic messages to send university information must be in accordance with applicable university data protection policies.

3) Mass Mailings – Employees that have a university-related business need to distribute messages to a large number of recipients (100+) through use of their University Account Mailbox should work with the component university's IT department in advance to ensure the messages are distributed appropriately. Mass mailings attempted without prior approval may be flagged as spam messages and subject to delay or deletion. Employees are responsible for complying with applicable component university requirements regarding message format and content. Official university contact information for the sender must be included in all distributed messages.

5. REVIEW AND RESPONSIBILITY

Responsible Party:	Associate Vice Chancellor for Information Technology
Review:	Every three years on or before June 1

6. APPROVAL

Approved: Jim McShan
Interim Vice Chancellor for Administration and Finance

Renu Khator
Chancellor

Date: March 25, 2016

REVISION LOG

Revision Number	**Approval Date**	**Description of Changes**
1	06/12/2015	Initial version
2	03/25/2016	Changed the Section in SAM 07.A.07 from "Information Services" to "Information Technology." No other changes were indicated by the Subject Matter Expert (SME)