

**THE TEXAS A&M UNIVERSITY SYSTEM
HEALTH SCIENCE CENTER INTERNAL POLICIES**

29.01.03.Z1.06 Email

Approved March 16, 2011

Supplements System Regulation 29.01.03

1. GENERAL

1.1 Introduction

Under the provisions of Texas Government Code §2054, the Information Resources Management Act, information resources are strategic assets of the State of Texas that must be managed as valuable state resources. Thus this policy is established to achieve the following:

- Ensure compliance with applicable statutes, regulations, and mandates regarding the management of information resources.
- Establish prudent and acceptable practices regarding the use of email.
- Educate individuals using email with respect to their responsibilities associated with such use.

1.2 Audience

The Texas A&M University System Health Science Center (HSC) Email Policy applies equally to all individuals granted access privileges to any HSC information resource with the capacity to send, receive, or store electronic mail.

1.3 Definitions

- **Information Resources (IR):** any and all computer printouts, online display devices, magnetic storage media, and all computer-related activities involving any device capable of receiving email, browsing Web sites, or otherwise capable of receiving, storing, managing, or transmitting electronic data including, but not limited to, mainframes, servers, personal computers, notebook computers, hand-held computers, personal digital assistant (PDA), pagers, distributed processing systems, network attached and computer controlled medical and laboratory equipment (i.e. embedded technology), telecommunication resources, network environments, telephones, fax machines, printers and service bureaus. Additionally, it is the procedures, equipment, facilities, and software that are designed, built, operated, and maintained to create, collect, record, process, store, retrieve, display, and transmit information.

- **Electronic mail system:** Any computer software application that allows electronic mail to be communicated from one computing system to another.
- **Electronic mail (email):** Any message, image, form, attachment, data, or other communication sent, received, or stored within an electronic mail system.

2. E-MAIL POLICY

2.1 The following activities are prohibited:

- Sending email that is intimidating or harassing.
- Using email to conduct personal business, with the exception of incidental use.
- Using email for purposes of political lobbying or campaigning.
- Violating copyright laws by inappropriately distributing protected works.
- Posing as anyone other than oneself when sending email, except when authorized to send messages for another when serving in an administrative support role.
- The use of unauthorized e-mail software.

2.2 The following activities are prohibited because they impede the functioning of network communications and the efficient operations of electronic mail systems:

- Sending or forwarding chain letters.
- Sending unsolicited messages to large groups except as required to conduct Institution business.
- Sending excessively large messages
- Knowingly sending or forwarding email that is likely to contain a computer virus.

2.3 All sensitive HSC material transmitted over external network must be encrypted.

2.4 All user activity on HSC information resources assets is subject to logging and review.

2.5 Electronic mail users must not give the impression that they are representing, giving opinions, or otherwise making statements on behalf of HSC or any unit of the HSC unless appropriately authorized (explicitly or implicitly) to do so. Where appropriate, an explicit disclaimer will be included unless it is clear from the context that the author is not representing the HSC. An example of a simple disclaimer is: "the opinions expressed are my own, and not necessarily those of my employer."

2.6 Individuals must not send, forward or receive confidential or sensitive HSC information through non-HSC email accounts. Examples of non-HSC email

accounts include, but are not limited to, Hotmail, Yahoo mail, AOL mail, and email provided by other Internet Service Providers (ISP).

2.7 Individuals must not send, forward, receive or store confidential or sensitive HSC information utilizing non-HSC accredited mobile devices. Any non-HSC accredited mobile devices will be listed on the Office of Information Technology website.

3. DISCIPLINARY ACTIONS

Violations of this policy may result in disciplinary action which may include termination for employees and temporary workers; a termination of employment relations in the case of contractors or consultants; dismissal for interns and volunteers; or suspension or expulsion in the case of a student. Additionally, individuals are subject to loss of HSC information resources access privileges, civil, and criminal prosecution.

OFFICE OF RESPONSIBILITY

Vice President Finance and Administration