



TEXAS SOUTHERN UNIVERSITY
MANUAL OF ADMINISTRATIVE POLICIES AND PROCEDURES

SECTION: Information Technology
AREA: Computer And Information Technology

Policy 04.06.10

SUBJECT: Email Policy

I. PURPOSE & SCOPE

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

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

This policy establishes rules for sending, receiving, or storing electronic mail. To the extent this policy conflicts with existing University policy, the existing policy is superseded by this policy. The Email Policy applies equally to all individuals granted access privileges to any University information resource with the capacity to send, receive, or store electronic mail.

II. POLICY PROVISIONS

- A. The following activities are prohibited by policy:
 - 1. Sending email that is intimidating or harassing.
 - 2. Using email for conducting personal business.
 - 3. Using email for purposes of political lobbying or campaigning.
 - 4. Violating copyright laws by inappropriately distributing protected works.
 - 5. Posing as anyone other than oneself when sending email, except when authorized to send messages for another when serving in an administrative support role.
 - 6. The use of unauthorized e-mail software.

- B. The following activities are prohibited because they impede the functioning of network communications and the efficient operations of electronic mail systems:
 - 1. Sending or forwarding chain letters.
 - 2. Sending unsolicited messages to large groups except as required to conduct University business.

3. Sending excessively large messages except as required to conduct University business.
 4. Sending or forwarding email that is likely to contain computer viruses.
- C. All sensitive University material transmitted over external network must be encrypted.
- D. All user activity on University information resources and technology assets is subject to logging and review.
- E. Electronic mail users must not give the impression that they are representing, giving opinions, or otherwise making statements on behalf of University or any unit of the University 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 University. An example of a simple disclaimer is "the opinions expressed are my own, and not necessarily those of my employer."
- F. Individuals must not send, forward or receive confidential or sensitive University information through non-University email accounts. Examples of non-University email accounts include, but are not limited to, Hotmail, Yahoo mail, AOL mail, and email provided by other Internet Service Providers (ISP).
- G. Individuals must not send, forward, receive or store confidential or sensitive University information utilizing non-University accredited mobile devices. Examples of mobile devices include, but are not limited to, Personal Data Assistants (PDA), two-way pagers and cellular telephones.

III. DISCIPLINARY ACTION

Violation of this policy may result in immediate disciplinary action pursuant to University policy (MAPP 02.05.03 – Discipline & Termination Policy).

IV. APPLICABLE TSU SECURITY POLICY STANDARDS

All individuals with authorized access to any TSU information resource and technology, including staff, faculty, students, consultants, contractors and volunteers, must adhere to all provisions of this policy, as well as applicable security standards included in the Security Standards Policy – MAPP 04.06.22). Applicable security standards include, but are not limited to:

- Security Standard 3
- Security Standard 6
- Security Standard 7
- Security Standard 8

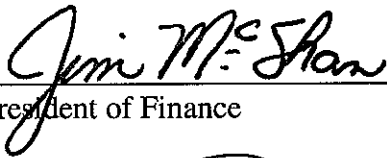
V. REVIEW AND RESPONSIBILITIES

Responsible Party: Chief Information Officer

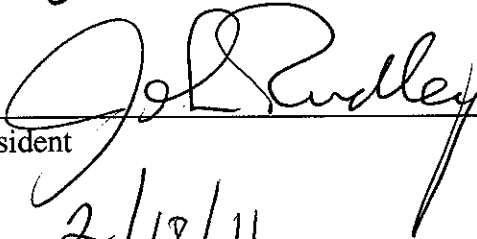


Review: Every year, on or before September 1

VI. APPROVAL



Vice President of Finance



President

2/18/11

Effective Date