I. PURPOSE AND SCOPE

Pursuant to 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. Accordingly, 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 University email; and
C. Inform individuals of their responsibilities associated with the use of University email.

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 To the extent this policy conflicts with existing University policy, the existing policy is superseded by this policy.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. DEFINITIONS

Not applicable.

III. POLICY PROVISIONS

Prohibited Activities

1. The following activities are prohibited by policy:
    1.1. Sending intimidating or harassing email.
    1.2. Using email to conduct personal business. Limited incidental personal use is permitted, provided such use is infrequent, does not interfere with University operations, does not consume significant resources, and complies with all applicable University policies.
    1.3. Using email for purposes of political lobbying or campaigning.
    1.4. Violating copyright laws by inappropriately distributing protected works.
    1.5. Posing as anyone other than oneself when sending email, except when authorized to send messages for another when serving in an administrative support role.
    1.6. Using unauthorized e-mail software.

2. The following activities are prohibited because they impede the functioning of network communications and the efficient operations of electronic mail systems:
    2.1. Sending or forwarding chain letters.
    2.2. Sending unsolicited messages to large groups except as required to conduct University business.
    2.3. Sending excessively large messages except as required to conduct University business.
    2.4. Sending or forwarding email that is likely to contain computer viruses or phishing technologies.

3. All sensitive University material transmitted over an external network must be encrypted.

4. All user activity on University information resources and technology assets is subject to logging and review. University employees with electronic mail addresses have no expectation of privacy regarding the information sent to and received from the email address.

5. Electronic mail users must not give the impression that they are representing, giving opinions, or otherwise making statements on behalf of the University or any unit of the University unless appropriately authorized (explicitly or implicitly) to do so. Where appropriate, an explicit disclaimer must 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.

6. 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, Gmail, Yahoo Mail, and email provided by other mail services.

7. The University understands and will comply with its obligation to preserve emails during litigation, internal and external investigations and audits as outlined in a Litigation Hold or preservation of evidence directive, regardless of University records retention policies.
8. Disciplinary Action

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

9. 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:

i Security Standard 3
ii Security Standard 6
iii Security Standard 7