TEXAS A&M **INTERNATIONAL** UNIVERSITY

Standard Administrative Procedure (SAP)

29.01.99.L1.07 Email

First Approved: March 28, 2013
Revised: October 20, 2017
Next Scheduled Review: October 20, 2022

Procedure Statement and Reason for Procedure

Under the provisions of the Information Resources Management Act, information resources are strategic assets of the State of Texas that must be managed as valuable State resources.

The purpose of this SAP is to ensure compliance with applicable statutes, regulations, and mandates regarding the management of information resources; to establish the rules for sending, receiving, or storing Texas A&M International University (TAMIU) electronic mail; and to educate individuals on the responsibilities assumed when using email. This SAP applies to all individuals granted access privileges to any TAMIU Information Resource with the capacity to send, receive, or store electronic mail, and supplements *TAMIU Rule 29.01.99.L1, Information Resources*.

Procedures and Responsibilities

1. Email Usage

    1.1 Email must be used in a manner that achieves its purpose without exposing TAMIU to any technical, financial, reputational, or legal risks.

    1.2 TAMIU has implemented an automated email retention schedule on the email servers. It is the responsibility of each user to retain emails in accordance with the State of Texas records retention policy.

1.3 TAMIU email accounts are an official communication channel for TAMIU business. Individuals must not use personal email accounts for official TAMIU business. Such use may require the employee to surrender information contained within personal email accounts pertinent to open records requests and may result in disciplinary action up to and including termination.

1.4 All user activity on TAMIU Information Resource assets is subject to logging and review. There should be no expectation of privacy.

2. Prohibited Email Usage

2.1 The following activities are prohibited:

2.1.1 Sending email that is intimidating or harassing.
2.1.2 Using email for conducting non-approved, private, commercial purposes.
2.1.3 Using email for purposes of political lobbying or campaigning.
2.1.4 Violating copyright laws by inappropriately distributing protected works.
2.1.5 Posing as anyone other than oneself when sending email, except when authorized to send messages for another individual while serving in an administrative support role.

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

2.2.1 Sending or forwarding chain letters.
2.2.2 Sending unsolicited messages to large groups except as required to conduct TAMIU business.
2.2.3 Sending excessively large messages.
2.2.4 Sending or forwarding email that is likely to contain computer viruses.

2.3 Electronic mail users must not give the impression that they are representing, giving opinions, or otherwise making statements on behalf of TAMIU or any unit of TAMIU 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 TAMIU. An example of a simple disclaimer is: "The opinions expressed are my own, and not necessarily those of my employer."

2.4 Individuals must not send confidential or sensitive TAMIU information through email accounts (refer to *TAMIU SAP 29.01.99.L1.31, Information Classification*) without appropriate safeguards or risk mitigation measures such as encryption. If transmission of confidential or sensitive information to third parties is absolutely necessary, it must be secured (e.g., encrypted or using secured file transfer services) and sent to their official, individual, company/organization email account.

Related Statutes, Policies, Regulations, or Rules

TAC, Chapter 202, Subchapter C, Information Security Standards for Institutions of Higher Education
System Policy 29.01, Information Resources
TAMIU Rule 29.01.99.L1, Information Resources
TAMIU SAP 29.01.99.L1.31, Information Classification

Appendix

References:
Copyright Act of 1976
Foreign Corrupt Practices Act of 1977
Computer Fraud and Abuse Act of 1986
Computer Security Act of 1987
The Health Insurance Portability and Accountability Act of 1996 (HIPAA)The State of Texas Information Act
Texas Government Code, Section 441
Texas Administrative Code, Chapter 202
IRM Act, 2054.075(b)
The State of Texas Penal Code, Chapters 33 and 33A
DIR Practices for Protecting Information Resources Assets
DIR Standards Review and Recommendations Publications

Contact Office

Office of Information Technology, 956-326-2310