STANDARD ADMINISTRATIVE PROCEDURE

29.01.03.M0.07 Information Resources – Enterprise Email Services

Approved September 16, 2010
Revised June 23, 2015
Revised November 19, 2019
Next scheduled review: November 19, 2024

Standard Administrative Procedure Statement

Electronic mail (email) services are provided by Texas A&M University (Texas A&M) for the purpose of enhancing productivity and maintaining effective communications in support of the Texas A&M mission. Texas A&M encourages the use of email for the distribution of information to faculty, staff, and students.

Definitions

University Electronic Directory – also known as Enterprise Directory which is used to manage NetID accounts and email account aliases for:

- personnel with an active, close affiliation to the university;
- retirees
- former students;
- guests and parents; and
- organizations and roles.

Enterprise Email Services – Email services (address routing and mailbox services) provided or managed by the Division of Information Technology.

Responsibilities and Procedures

1. APPLICABILITY

    1.1 This procedure applies to all users of Texas A&M enterprise email services.

2. RESPONSIBILITIES

2.1 Use of university provided email resources and the content of email messages must be in accordance with SAP 29.01.03.M0.02 *Acceptable Use* and all applicable state or federal laws.

2.2 Each Texas A&M University employee who has email access associated with their employment is responsible for claiming their entry in the university electronic directory and for keeping their directory information current.

2.3 Each employee is expected to check email messages for university-related communications on a frequent and consistent basis.

2.4 All units at Texas A&M that handle Protected Health Information (PHI) must ensure that email communications about PHI comply with the Health Insurance Portability and Accountability Act (HIPAA) and State of Texas requirements to protect individual's confidential information.

3. UNIVERSITY ELECTRONIC DIRECTORY AND EMAIL SERVICES

3.1 The university electronic directory is the primary directory for Texas A&M related email communications. All email addressed in the form identifier@tamu.edu is checked against this directory to determine where to ultimately deliver the message.

3.2 All employees are automatically listed in the university directory. When necessary, and with appropriate authorizing documents, directory information can be suppressed.

3.3 Texas A&M Division of Information Technology manages enterprise email services that are available for use by all university employees as well as enrolled students.

3.3.1 Enterprise email services may be offered to affiliates of the university (i.e., visiting scholars, vendors, former employees) upon request and approval by a departmental sponsor and the Associate Vice President and Chief Information Security Officer (CISO) or designee. Sponsored email services will only be valid for a period of one year, and must be renewed annually.

3.3.2 Employee email services will be decommissioned a maximum of 72 hours after the date of termination.

3.3.3 Student email services will be decommissioned a maximum of two years after the date of last enrollment.

3.4 Email messages are electronically scanned and filtered according to processes managed by the office of the CISO.

3.4.1 Messages that are determined to contain malicious content (i.e., viruses, malware, or phishing attempts) may be rejected.

3.4.2 Messages that are likely to be spam are quarantined or discarded. Users can access their own message quarantine to release or delete flagged messages, or to manage the behavior of the spam filtering system for their mailbox.

4. EMAILS SUBJECT TO DISCLOSURE

4.1 University employees should have no expectation of privacy in the use of email for university business. Email messages that are maintained by the university and its employees or contractors, and which are related to university business, are subject to the Texas Public Information Act (TPIA).

4.2 Employee and student email messages may be subject to disclosure for audits, investigations, regulatory, or legal proceedings.

4.3 Private email accounts shall not be used for conducting university business. The university may require an employee to disclose any email messages residing in an employee's private email account(s) relating to university business to satisfy obligations under TPIA, an audit, investigation, legal or official proceeding. An employee failing to comply with such a request from the university will be subject to disciplinary action, up to and including dismissal.

5. EMAIL AND RECORDS RETENTION

5.1 The content and function of an email message determines whether it is a state record. Only email messages that meet the criteria for state records are subject to records retention requirements. An email message is not a state record unless the message uniquely documents university business and is NOT merely a convenience copy (University Records Management and The Texas A&M System Records Retention Schedule).

5.2 Employees leaving a position may be required to review their email account with their supervisor. The supervisor is responsible for ensuring that any electronic messages are properly stored or disposed.

6. COMPLIANCE AND PROHIBITED ACTIVITIES

6.1 Use of email resources and the content of email messages must be in compliance with all applicable state and federal laws and regulations as well as all university Rules, SAPs, and information security controls.

6.2 Users of university provided email services shall not abuse the privilege of access to university information resources (reference SAP 29.01.03.M0.02 *Acceptable Use*).

7. EMAIL SERVICES NOT MANAGED BY THE DIVISION OF IT

7.1 Administrative units that deploy alternative email systems are responsible for the administration of such systems. All use must be in accordance with this Standard Administrative Procedure.

Related Statutes, Policies, Requirements, or Procedures

Health Insurance Portability and Accountability Act (HIPAA)

Texas Public Information Act

System Policy 33.04 *Use of System Resources*

System Regulation 61.99.01 *Retention of State Records*

SAP 29.01.03.M0.02, *Acceptable Use*

SAP 61.99.01.M0.01, *Records Management*

Texas A&M University System Records Retention Schedule

Contact Office

Office of the Chief Information Security Officer

Office of Responsibility: Vice President for Information Technology and Chief Information Officer