Texas A&M University System Offices Standard
Employee Instant Messaging

Approved September 4, 2019
Next Scheduled Review: September 4, 2022

Standard Statement

Instant messaging (IM) services are supported by The Texas A&M University System (system) and System Offices ("System Offices") for the purpose of enhancing productivity and maintaining effective communications in support of the System Offices mission. The System Offices encourages the secure use of IM for the distribution of certain information to System Offices employees.

Definitions

Instant Messaging (IM) – the exchange of near, real-time messages through a stand-alone application or embedded software. Instant messaging provides users with the ability to see whether a co-worker is online and connected (presence) and to share text, files, and images.

Official Procedure and Responsibilities

1. APPLICABILITY

   This standard applies to all System Offices employees.

2. RESPONSIBILITIES

   2.1 The use of IM resources and the content of IM messages must be in accordance with the System Offices *Standard for Acceptable Use*, the System Offices *Standard for Data Classification and Data Protection*, and all applicable state or federal laws.

   2.2 Each System Offices employee who has IM access associated with their employment is responsible for keeping their directory information current.

   2.3 Each employee is expected to check IM messages for system-related communications on a frequent and consistent basis. The system recommends checking IM messages at least once per hour.

2.4 All units at the System Offices that handle Protected Health Information (PHI) must ensure that IM communications about PHI comply with the Health Insurance Portability and Accountability Act (HIPAA) and state of Texas requirements to protect individuals' confidential information. They must also observe the System Offices *Standard for Data Classification and Data Protection*.

3. IMs SUBJECT TO DISCLOSURE

3.1 System Offices-provided IM services should be used only for system business, and there is no expectation of privacy in the use of System Offices-provided IM services or other IM services for messages relating to system business. IMs that are maintained by the system and its employees or contractors, and which are related to system business, are subject to the Texas Public Information Act (TPIA).

3.2 Employee IMs may also be subject to disclosure for audits, investigations, regulatory, or legal proceedings.

3.3 Private IM accounts should not be used for conducting system business. The System Offices may require an employee to disclose any IMs residing in an employee's private IM account(s) relating to system business to satisfy obligations under TPIA, an audit, investigation, regulatory, or legal proceeding. An employee failing to comply with such a request from the system will be subject to disciplinary action, up to and including dismissal.

4. IMs AND RECORDS RETENTION

4.1 The content and function of an IM determines whether it is a state record. Only IMs that meet the criteria for state records are subject to records retention requirements. An IM is not a state record unless the message uniquely documents system business and is NOT merely a convenience copy or transitory information. Any IM that is a state record must be retained in an appropriate electronic records management system (not in an IM account), in accordance with system records retention requirements.

4.2 The use of System Offices-provided IM services should be limited to the sharing of short-term messages requiring immediate action or confirmation of presence. Information of an enduring nature (in this case, required after 48 hours) should utilize email messaging services or other storage provided by the system.

4.3 IMs utilizing a System Offices-provided IM service will only be retained for 24 hours or the minimum retention offered in the configuration of the IM service (whichever is shorter).

5. COMPLIANCE AND PROHIBITED ACTIVITIES

5.1 The use of IM resources and the content of IMs must be in compliance with all applicable state and federal laws and regulations as well as all system policies and procedures.

5.2 The use of System Offices-provided IM services must comply with all System Offices Rules and Standard Administrative Procedures.

5.3 Users of System Offices-provided IM services shall not abuse the privilege of access to system information resources (See the System Offices *Standard for Acceptable Use*.

6. ALTERNATE IM SERVICES

6.1 Only System Offices-provided IM services should be used for conducting system business; alternate IM accounts (i.e., alternate IM accounts in addition to private IM accounts) are not authorized for conducting system business. The system may require an employee to disclose any IMs residing in an alternate IM account(s) relating to system business to satisfy obligations under TPIA, an audit, investigation, legal or official proceeding. An employee failing to comply with such a request from the system will be subject to disciplinary action, up to and including dismissal.

Related Statutes, Policies, Requirements or Procedures

Health Insurance Portability and Accountability Act (HIPAA)

Texas Public Information Act

System Regulation *29.01.03, Information Security*

System Policy *33.04, Use of System Resources*

System Regulation *61.99.01, Retention of State Records*

The Texas A&M University System Records Retention Schedule

Contact Office

For interpretation or clarification, contact The Texas A&M University System Chief Information Security Officer.

OFFICE OF RESPONSIBILITY: The Texas A&M University System Chief Information Officer