29.01.03.H0.04 Email Use

Approved: April, 2014
Next Scheduled Review: April, 2019

Procedure Statement

The University assigned email account is the University's official means of email communication with students, faculty, and staff at Texas A&M University-Texarkana. Individuals are responsible for all information sent to them via their University assigned email account. The University expects that University email communications will be read in a timely manner.

Reason for Regulation

- Required by Texas Administrative Code Section 202
- This Standard Administrative Procedure (SAP) applies to University information resources that store or process mission critical and/or confidential information.
- The purpose of the implementation of this SAP is to provide a set of measures that will mitigate information security risks associated with email. There may also be other or additional measures that will provide appropriate mitigation of the risks. The assessment of potential risks and the application of appropriate mitigation measures are to be determined by the information resource owner or their designee. In accordance with Texas Administrative Code 202 - Information Security Standards, each department and/or resource owner may elect not to implement some or all of the risk mitigation measures provided in this SAP based on information security risk management decisions and business functions. Such risk management decisions must be documented and reported to the designated Information Security Officer (ISO).
- The intended audience for this standard administrative procedure includes, but is not limited to, all information resources data/owners, users, management personnel, students and system administrators.

Procedures and Responsibilities

1. University use of email

1.1. Assignment of email addresses: Information Technology (IT) will assign students, faculty, and staff an official University email address.

1.2. Redirecting of email: The University will not be responsible for the handling of email by third parties (e.g. Yahoo, AOL, Gmail, Hotmail, etc). Having email redirected does not release a student, faculty member or staff member from the responsibilities associated with communication sent to his or her official University email address.

1.3. Expectations regarding use of email: Students, faculty, and staff are expected to check their official email address on a frequent and consistent basis in order to stay current with University communications.

1.4. Backups of emails stored on central University email servers: Backups of email stored on central University email servers managed by Information Technology shall be retained by the University for 14 days.

2. Appropriate use of email: The following activities are prohibited.

2.1. Sending email that is intimidating or harassing

2.2. Using email for conducting personal business

2.3. Using email for purposes of political lobbying or campaigning

2.4. Violating copyright laws by inappropriately distributing protected works

2.5. Posing as anyone other than oneself when sending email, except when authorized to send messages for another when serving in an administrative support role

2.6. The use of unauthorized email software

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

3.1 Sending or forwarding chain letters

3.2 Sending unsolicited messages to large groups except as required to conduct Texas A&M University-Texarkana business

3.3 Sending excessively large messages

3.4 Sending or forwarding email that is likely to contain computer viruses

4. All sensitive and/or confidential Texas A&M University-Texarkana material transmitted over external network should be encrypted.

   4.1. In general, email is not appropriate for transmitting sensitive or confidential information.

   4.2. Confidentiality regarding student records is protected under the Family Educational Rights and Privacy Act of 1974 (FERPA). All use of email, including use for sensitive or confidential information, will be consistent with FERPA.

5. All user activity on Texas A&M University-Texarkana information resources assets is subject to logging and review.

6. Electronic mail users must not give the impression that they are representing, giving opinions, or otherwise making statements on behalf of Texas A&M University-Texarkana or any unit of Texas A&M University-Texarkana 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 Texas A&M University-Texarkana. An example of a simple disclaimer is: "the opinions expressed are my own, and not necessarily those of my employer."

7. Individuals must not send, forward or receive confidential or sensitive Texas A&M University-Texarkana information through non-Texas A&M University-Texarkana email accounts. Examples of non-Texas A&M University-Texarkana email accounts include, but are not limited to: Yahoo, AOL, Gmail, Hotmail and email provided by other Internet Service Providers (ISPs).

Related Statutes, Policies, or Requirements

- Texas Administrative Code Section 202

Definitions

Information Resources (IR): the procedures, equipment, and software that are designed, employed, operated, and maintained to collect, record, process, store, retrieve, display, and transmit information or data.

Information Security Officer (ISO): responsible for administering the information security functions within Texas A&M University-Texarkana and reports to the Information Resources Manager (IRM).

Mission Critical Information: information that is defined by the University or information resource owner to be essential to the continued performance of the mission of the University or

department. Unavailability of such information would result in more than an inconvenience. An event causing the unavailability of mission critical information would result in consequences such as significant financial loss, institutional embarrassment, failure to comply with regulations or legal obligations, or closure of the University or department.

Data: shall include all information that is used by or belongs to the University or that is processed, stored, maintained, transmitted, copied on, or copied from University computing resources.

Forged communications: (sometimes referred to as "spoofing") shall be defined as emails that are made to appear as if they originated from an organization or individual other than the individual from whom the message was actually sent.

Protected information: shall be defined as data that has been designated as private, protected, or confidential by law or by the University. Protected information includes, but is not limited to, employment records, medical records, student records, education records, personal financial records (or other individually identifiable information), research data, trade secrets, and classified government information.

Protected information shall not include public records that by law must be made available to the general public. To the extent there is any uncertainty as to whether any data constitutes protected information, the data in question shall be treated as protected information until a determination is made by the University.

Contact Office

Contact Office: Department of Information Technology, 903-223-3084