The Division of Information Technology
University Information Security Standards

Information Security Standard – Email Communications (Legacy TAC 202)
Approved: April 15, 2005
Last Revised: July 26, 2017
Next Scheduled Review: August 2018

Supplements the following:

- Information Resources - Security of Electronic Information Resources, 24.99.99.W1/PR
- Information Resources – Rules for Responsible Information Technology Usage, 33.04.99.W1/PR

1. General

University information resources are strategic assets and as such must be managed as valuable state resources. Since a large portion of University business is conducted using email, it is imperative that email services function in an efficient and reliable manner. These procedures, therefore, address expected standards for University email usage. This policy is established to achieve the following:

- To ensure compliance with applicable statutes, regulations, and mandates regarding the management of information resources.
- To establish prudent and acceptable practices regarding the use of email.
- To educate individuals using email with respect to their responsibilities associated with such use.

2. Applicability

This standard provides procedures regarding the use of email through University owned information resources.

The purpose of this standard is to provide a set of measures that will mitigate information security risks associated with email use. The university assigned account is the university's official means of email communication with students, faculty, and staff at West Texas A&M University. 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.

The West Texas A&M University email policy applies equally to all individuals granted access privileges to any West Texas A&M University information resource with the capacity to send, receive, or store electronic mail.

3. Definitions

3.1 Confidential Information: information that is excepted from disclosure requirements under the provisions of applicable state or federal law, e.g., the Texas Public Information Act.

3.2 Information Resources: Any and all computer printouts, online display devices, magnetic storage media, and all computer-related activities involving any device capable of receiving email, browsing Web sites, or otherwise capable of receiving, storing, managing, or transmitting electronic data including, but not limited to, mainframes, servers, personal computers, notebook computers, hand-held computers, personal digital assistant (PDA), pagers, distributed processing systems, network attached and computer controlled medical and laboratory equipment (i.e. embedded technology), telecommunication resources, network environments, telephones, fax machines, printers and service bureaus. Additionally, it is the procedures, equipment, facilities, software, and data that are designed, built, operated, and maintained to create, collect, record, process, store, retrieve, display, and transmit information.

3.3 Information Resources Manager (IRM): Responsible to the State of Texas for management of the agency/university's information resources. The designation of an agency/university information resources manager is intended to establish clear accountability for setting policy for information resources management activities, provide for greater coordination of the state agency's information activities, and ensure greater visibility of such activities within and between state agencies. The IRM has been given the authority and the accountability by the State of Texas to implement Security Policies, Procedures, Practice Standards, and Guidelines to protect the Information Resources of the agency. If an agency does not designate an IRM, the title defaults to the agency's Executive Director, and the Executive Director is responsible for adhering to the duties and requirements of an IRM.

3.4 Information Security Officer (ISO): Responsible to the executive management for administering the information security function within the agency. The ISO is the university's internal and external point of contact for all information security matters.

3.5 User: An individual or automated application or process that is authorized to the resource by the owner, in accordance with the owner's procedures and rules.

4. Procedures

4.1 Email should be limited to the intended purpose for which the logon ID was issued, except when used as defined by incidental use. Refer to Rules for Responsible Information Technology Usage, 33.04.99.W1.

4.2 Email is an official means of communication within West Texas A&M University. Therefore, the university will use the WTAMU issued account to send communications to students, faculty, and staff via email. The university expects that those communications will be read in a timely manner.

4.3 The office of information technology will assign students, faculty, and staff an official university email address.

4.4 The university will not be responsible for handling of email by third parties (e.g. local mail servers, Yahoo Mail, Gmail, Hotmail, etc). Having email directed does not release a student, faculty or staff members from the responsibilities associated with communication sent to his or her official university email address.

4.4 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.

4.5 Backups of email stored on central university email servers managed by information technology shall be retained by the university for 6 months.

5. Appropriate use of email

5.1 The following activities are prohibited:

- Sending email that is intimidating or harassing
- Using email for conducting personal business
- Using email for purposes of political lobbying or campaigning
- Violating copyright laws by inappropriately distributing protected works
- Posing as anyone other than oneself when sending email, except when authorized to send messages for another when serving in an administrative support role
- The use of unauthorized email software

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

- Sending or forwarding chain letters

- Sending unsolicited messages to large groups except as required to conduct West Texas A&M University business
- Sending excessively large messages
- Sending or forwarding email that is likely to contain computer viruses

5.3 All sensitive and/or confidential West Texas A&M University material transmitted over external networks must be encrypted. Email is not appropriate for transmitting sensitive or confidential information unless it is encrypted.

- 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.

5.3 All user activity on West Texas A&M University information resources assets is subject to logging and review.

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

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

OFFICE OF RESPONSIBILITY: Information Technology

CONTACT: Chief Information Officer