The Division of Information Technology
University Information Security Standards

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

1. General

Understanding the importance of information security and individual responsibilities and accountability pertaining to information security are paramount to achieving University security goals. This can be accomplished with a combination of general information security awareness training and targeted, product-specific training. The security awareness and training information needs to be ongoing and updated as needed. The purpose of security training is to describe the requirements to ensure each user of university information resources receives adequate training on information security issues.

2. Applicability

This information security standard applies to all users of University information resources.

The purpose of this information security standard is to provide a set of measures that will mitigate information security risks associated with Security Awareness and Training. There may also be other or additional measures that department heads or deans will provide to further mitigate risks. The assessment of potential risks and the application of appropriate mitigation measures is to be determined by the department heads and their identified information security administrators. 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 is based on documented information security risk management decisions and business functions. Such risk management decisions must be documented and approved by the designated Information Security Officer (ISO).

The intended audience is all users of information resources.

3. Definitions

3.1 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.

3.2 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.

3.3 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.

3.4 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, and failure to comply with regulations or legal obligations, or closure of the University or department.

4. Procedure

4.1 All West Texas A&M University personnel who use information resources are required to comply with the procedures outlined in this information security standard. A method to accomplish the requirements listed below is provided through the use of the Information Security Awareness (ISA) training module. This web-based training module is access via the Single-Sign-On (SSO) located at http://sso.tamu.edu. The module is one of the offerings listed in the training section.

4.2 All new employees shall complete security awareness training prior to, or at least within 30 days of, being granted access to any University information resources. This shall be part of the new employee's orientation training session.

4.3 All users must acknowledge they have read, understand, and will comply with the university requirements regarding computer security policies and procedures.

4.4 All users shall acknowledge completion of university security awareness training on an annual basis.

4.5 Departments may require additional incidental training and require acknowledgement as determined by the department.

4.6 Departmental information technology personnel shall establish and maintain a process to communicate new security program information, security bulletin information, and security items of interest to departmental personnel.

4.7 All departmental information security administrators shall ensure their personnel's completion of security awareness training on an annual basis, provided through HRConnect. Department Heads may require additional incidental training and require acknowledgement of their personnel as they see fit.

OFFICE OF RESPONSIBILITY: Information Technology

CONTACT: Chief Information Officer