29.01.03.H0.20 Security Awareness

Approved: April 2014
Revised: January 5, 2024
Next Scheduled Review: January 2029

Procedure Summary

Understanding the importance of information security and individual responsibilities and accountability pertaining to information security are paramount to achieving organization 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 the security training procedure is to describe the requirements to ensure each user of university information resources receives adequate training on information security issues.

The purpose of the implementation of this Procedure is to provide a set of measures that will mitigate information security risks associated with security awareness. There may also beother or additional measures that will provide appropriate mitigation of the risks. The assessment of potential risks and the application of appropriate mitigation measures are tobe 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 procedure 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).

Procedures and Responsibilities

1. All Texas A&M University-Texarkana (TAMUT) personnel who use information resources are required to comply with the procedures outlined in this procedure. A method to accomplish therequirements listed below is provided through the use of the Information Security Awareness (ISA) training module (Course 3001). This web-based training module is accessed via Single Sign On's TrainTraq.

    1.1. All new employees shall complete security awareness training within 30 days of being granted access to any TAMUT information resources. This shall be part of the new employee's orientation training.

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

1.3. In accordance with the University Procedure29.01.03.H0.02, *Acceptable Use*, users are responsible for safeguarding their TAMUT account(s), passwords, Personal Identification Numbers (PIN), Identification Cards, or similar information or devices used for identification and authorization purposes. Sharing of such information or devices with others is strictly prohibited.

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

1.4.1. Security awareness training shall address recognition and reporting of indicators for insider threats.

1.4.2. All employees must complete TrainTraq courses FERPA every 2 years, if applicable, and Information Security Awareness on a yearly basis in order to gain access to Confidential Information Resources.

1.4.3. Employees that do not complete their required training will have their access removed until SSO TrainTraq courses have been completed.

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

3. 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. Department heads shall ensure that personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.

Related Statutes, Policies, or Requirements

Texas Administrative Code Section 202
University Procedure29.01.03.H0.02, Acceptable Use

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.

Owner of an Information Resource: an entity responsible for a business function and for determining controls and access to information resources supporting that business function.

Information Security Officer (ISO): responsible for administering the information security functions within TAMUT 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.

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

Department of Information Technology
903-334-6603