Procedure Statement

Understanding the importance of information security, 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 is a continuous effort and will be 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.

Reason for Procedure

This procedure applies to all users of Texas A&M University – San Antonio (“The University”) information resources.

The purpose of the implementation of this procedure is to provide a set of measures that will mitigate information security risks associated with security training. There may also be other or additional measures that owners of information resources, department or division heads will provide to further mitigate risks. The assessment of potential risks and the application of appropriate mitigation measures are to be identified by the University ISO in collaboration with the Information Resource owners and/or department heads. 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 with documented acceptance of identified risk(s), notice to, and acknowledgment by the ISO (e.g. copy of documentation provided to ISO).

Official Responsibilities and Procedure

1. All University personnel who use information resources are required to comply with the procedures outlined in this procedure. All Department Heads and Information Resource Owners shall ensure completion of security awareness training on an annual basis, provided through SSO. Additional training may be required by the IRO and assigned to identified personnel as they see fit.
1.1. 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.

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

2. Information technology personnel shall establish security program in addition to making relevant security information available to owners and users of information resources.

3. The Information Resource Owners may oversee the preparation, maintenance, and distribution of information security manuals or supplemental information security training that describe how university rules and procedures relate to the security of departmentally owned information resources. All manuals and/or supplemental documents are to be provided to the University ISO for reference and proper records retention.

---

Non-Compliance

Any user who does not complete the required training within 30 days (initial or annual training) may have their accounts disabled until training can be completed.

---

Related Rules

- System Policy 29.01 Information Resources
- System Regulation 29.01.03 Security of Electronic Information

---

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 Resources Manager (IRM)** – The IRM ensures that all information resources are acquired appropriately, implemented effectively, and complies with regulations and agency policies. Per requirements of the State of Texas, each agency or institution of higher education must designate an IRM.

**Information Resource Owner** – an entity responsible for:
- A business function; and,
- Determining controls and access to information resources supporting that business function.
Information Security Officer (ISO) - Responsible to the executive management for administering the information security functions within the agency. The ISO is the university's internal and external point of contact for all information security matters.

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.

Contact Office

Information Technology Services – (210) 784-4357 (HELP)