29.01.99.K1.170 Security Training Procedure

Approved: April 1, 2004
Revised: April 25, 2013
Revised: April 2, 2019
Next Scheduled Review: April 2, 2024

Introduction

Understanding the importance of information resource security and individual responsibilities and accountability are paramount to achieving organization security goals at Texas A&M University- Kingsville (TAMUK). This can be accomplished with a combination of general information resource security awareness training and targeted, product specific training. The training on Information Security Awareness is provided in TrainTraq and updated by the Texas A&M University System.

Purpose

The purpose of this procedure is to describe the requirements to ensure each user of Information Resources receives adequate training on information resource security issues.

Audience

The procedure applies to individuals that use the University's Information Resources.

Security Training Procedure

1. New users must complete the required Information Security Awareness training prior to, or at least within 30 days of, being granted access to any Information Resources.
2. The Information Security Awareness training module must be re-taken annually.
    a   An email reminder will be sent to those that have not completed Information Security Awareness by the due date.
    b   If the Information Security Awareness training has not been completed within a week of the email reminder the person's account will be disabled.
        i   TrainTraq may be accessed from off-campus or from public access computers or by coming to College Hall 220.
        ii Once the training has been completed, a copy of the TrainTraq course transcript can be delivered to College Hall 220 or emailed to ttsecure@tamuk.edu.

    iii Priority will be given so that accounts that have been disabled will be reinstated within the next business day.

3. Employees are responsible for keeping up to date on rules and standard administrative procedures regarding Information Resources.
4. Additional training opportunities will be provided to allow users to properly protect Information Resources.

Disciplinary Actions

Violation of this procedure may result in disciplinary action up to and including termination for employees and temporaries; a termination of contract relations in the case of contractors or consultants; dismissal for interns and volunteers; or suspension or expulsion in the case of students. Additionally, individuals are subject to loss of TAMUK Information Resources access privileges, civil and criminal prosecution.

References

1. System Policy 29.01 Information Resources
2. Texas Administrative Code 202.75 Information Resources Security Safeguards
3. System Regulation 29.01.03 Electronic Information Services Access and Security

---

Contact Office

For More Information, Contact: iTech
MSC 185, 700 University Blvd., Kingsville, TX 78363-8202
Contact Phone: 361-593-2404

29.01.99.K1.170 Security Training Procedure