

Screen Locking Standard Administrative Procedure



Approved: February 13, 2019

Next Scheduled Review: February 13, 2024

Introduction

In an effort to protect confidential or sensitive information, the implementation of screen locking at Texas A&M University-Kingsville (TAMUK) is designed to prevent unauthorized access to the system by initiating a session lock after 15 minutes of inactivity.

Purpose

The purpose of this procedure is to provide guidance on the implementation of screen locking at TAMUK to prevent unauthorized access to systems.

Audience

This procedure applies to information resources on the TAMUK domain. It is the responsibility of the individual having confidential or sensitive information in their possession or under their direct control to ensure that appropriate risk mitigation measures are in place to protect data from unauthorized exposure.

Screen Locking Procedure

1. Screen locking will be enabled to lock the system after 15 minutes of inactivity.
 - a. iTech will set a Group Policy Object (GPO) to enable the screen lock option on employees' and requested computers.
 - b. Departments may request screen lock for additional computers such as student workers who handle confidential or sensitive information.
2. Users will need to enter their password to unlock their computer.
 - a. Switch user feature may be used for shared devices.

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. Copyright Act of 1976
 2. Computer Fraud and Abuse Act of 1986
 3. Computer Security Act of 1987
 4. DIR Practices for Protecting Information Resources Assets
 5. DIR Standards Review and Recommendations Publications
 6. Foreign Corrupt Practices Act of 1977
 7. The Health Insurance Portability and Accountability Act of 1996 (HIPAA)
 8. IRM Act, 2054.075(b)
 9. The State of Texas Information Act
 10. The State of Texas Penal Code, Chapters 33 and 33A
 11. Texas Administrative Code, Chapter 202
 12. Texas A&M University-Kingsville Acceptable Use Procedure 29.01.99.K1.010
 13. Texas Government Code, Section 441
 14. TAMU System Policy 29.01.03 Information Security
-

Contact Office

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