## Privacy Procedure

### Introduction

Privacy procedures are mechanisms used to establish the limits and expectations for the users of Texas A&M University-Kingsville (TAMUK) Information Resources. Users of system information resources should have no expectation of privacy with respect to the use of information resources, including but not limited to email and/or any electronic files created, used, stored, sent or received on system devices.

Information resources may be accessed as needed for purposes of information system administration and maintenance, resolution of technical problems, security monitoring, administrative review, compliance with court orders and System Internal Audit Department, State of Texas audits, Texas Administrative Codes and other TAMUK iTech procedures.

### Purpose

The purpose of this procedure is to communicate the privacy expectations to information resources users.

### Audience

This procedure applies to individuals who use any TAMUK Information Resource.

### Privacy Procedure

1. Electronic files created, sent, received, or stored on information resources owned, leased, administered, or otherwise under the custody and control of TAMUK are not private and may be accessed by TAMUK iTech employees at any time without knowledge of the information resource user or owner.
2. To manage systems and enforce security, TAMUK may log, review, and otherwise utilize information stored on or passing through its information resources systems in accordance with the provisions and safeguards provided in the Texas Administrative Code 202, Information Resource Standards.
    a. For these same purposes, TAMUK may also capture user activity such as telephone numbers dialed and web sites visited.
3. Users must report any weaknesses in TAMUK Information Resources security, any incidents of possible misuse or violation of this agreement to the Information Security Officer.
4. Users must not attempt to access any data or programs contained on TAMUK systems for which they do not have authorization or explicit consent.
5. Users who sign non-disclosure agreements (NDA) with non-university entities or agents must provide copies of the NDAs to the University Compliance Officer.

### Disciplinary Actions

Violation of this procedure may result in disciplinary action up to and including termination for employees and temporaries; a termination of employment relations in the case of contractors or consultants; dismissal for interns and volunteers; or suspension or expulsion in the case of a student. 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 Procedure 29.01.03.K1.010
13. Texas A&M University-Kingsville Procedure 29.01.04.K1.010
14. Texas Government Code, Section 441