## Introduction

Data Classification provides a framework for managing  data assets based on value and associated risks and for applying the appropriate levels of protection as required by state and federal law as well as proprietary, ethical, operational, and privacy considerations. Texas A&M University-Kingsville (TAMUK) data, whether electronic or printed, should be classified. The data owner, is responsible for data classification, and should classify data as Category I, Category II, or Category III as defined below. Consistent use of data classification reinforces the expected level of protection of TAMUK data assets.

## Purpose

The purpose of this standard is to provide a foundation for the development and implementation of necessary information resources security controls to protect information according to its value or risk. Information resources security standards, which define these information resources security controls and requirements, may include: document marking/labeling, release procedures, privacy, transmission requirements, printing protection, computer display protections, storage requirements, destruction methods, physical security requirements, access controls, backup requirements, transport procedures, encryption requirements, and incident reporting procedures.

## Exception

Information owned or under the control of the United States Government must comply with the federal classification authority and federal protection requirements.

## Disciplinary Actions

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

## Contact Office

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