Portable Computing Security Procedure

Introduction
Portable computing devices are becoming increasingly powerful and affordable. Their small size and functionality are making these devices ever more desirable to replace traditional desktop devices in a wide number of applications. However, the portability offered by these devices may increase the security exposure to groups at Texas A&M University-Kingsville (TAMUK) using the devices.

Purpose
The purpose of this procedure is to establish the rules for the use of mobile computing devices and their connection to the network. These rules are necessary to preserve the integrity, availability, and confidentiality of TAMUK information.

Audience
This procedure applies to individuals that utilize portable computing devices and access University Information Resources.

Definitions
Portable Computing Devices: Any easily portable device that is capable of receiving and/or transmitting data to and from information resources. These include, but are not limited to, laptops, notebook computers, handheld computers, PDAs, pagers, and smartphones.

Portable Computing Procedure
1. Portable computing devices must be password protected.
2. TAMUK critical or sensitive data should not be stored on portable computing devices. However, in the event that there is no alternative to local storage, all sensitive University data must be encrypted using approved encryption techniques.
   a. If encryption is not available, delete sensitive information.
3. TAMUK data must not be transmitted via wireless to or from a portable computing device unless approved wireless transmission protocols along with approved encryption techniques are utilized.
4. Unattended portable computing devices must be physically secure. This means they must be locked in an office, locked in a desk drawer or filing cabinet, or attached to a desk or cabinet via a cable lock system.
5. A lost or stolen portable computing device must be reported immediately to the Information Security 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
4. DIR Practices for Protecting Information Resources Assets
5. DIR Standards Review and Recommendations Publications
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