29.01.99.K1.140 Portable Computing Security Standard Administrative Procedure

Effective: April 1st, 2004
Revised: April 25th, 2013
Revised: March 28th, 2019
Next Scheduled Review: March 2024

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 computer 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.

Portable Computing Procedure

1. TAMUK confidential or sensitive data should not be stored on portable computing devices. However, in the event that there is no alternative to local storage, all confidential or sensitive University data must be encrypted using approved encryption techniques.
    a. TAMUK offers OneDrive and Syncplicity for secured cloud storage.
    b. The portable computing device must be password-protected using the security feature provided on the tool, and there must be no sharing of the password.

    c. Whenever there is no longer a job related need to access or store this confidential information, it must be deleted.
2. Portable devices connecting to the university network must have current operating system patches and current supported anti-virus software.
    a. All wireless devices are required to authenticate through the TAMUK network access control (NAC) appliance.
3. TAMUK confidential or sensitive 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. All remote access to confidential or sensitive information from a portable computing device shall utilize encryption techniques, such as Virtual Private Network (VPN), Secure Socket Layers (SSL), Secure File Transfer Protocol (SFTP), Hyper Text Transfer Protocol Secured (HTTPS), or Transport Layer Security (TLS).
5. Unattended portable computing devices owned by users shall be kept physically secure using means appropriate to the potential risk associated with the device.
6. Keep portable computing devices patched and updated. Install anti-virus software and a personal firewall where applicable.
7. 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 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. 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
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