Network Access Procedure

Introduction
The Texas A&M University-Kingsville (TAMUK) network infrastructure is provided as a central utility for all users of University Information Resources. It is important that the infrastructure, which includes cabling and the associated wired and wireless equipment, continues to develop with sufficient flexibility to meet (TAMUK) demands while at the same time remaining capable of exploiting anticipated developments in high speed networking technology to allow the future provisioning of enhanced user services.

Purpose
The purpose of this procedure is to establish the rules for the access and use of the network infrastructure. These rules are necessary to preserve the integrity, availability and confidentiality of TAMUK information.

Audience
This procedure applies to individuals with access to any University Information Resource.

Network Access Procedure
1. All TAMUK owned PCs and laptops must be joined to the TAMUK domain.
2. Users are permitted to use only those network addresses issued to them by iTech.
3. All remote access to TAMUK resources will be established only through protocols approved by iTech.
4. Bridging between two networks is prohibited. A device may not be connected to the TAMUK network and an external network simultaneously except through sanctioned Virtual Private Network connections.
5. Users must not extend or re-transmit network services in any way including by installing a router, switch, hub, or wireless access point to the TAMUK network.
6. Users must not install network hardware or software that provides network services without iTech approval.
7. Non-TAMUK computer systems that require network connectivity must conform to iTech standards.
8. Users must not download, install, or run security programs or utilities that reveal weaknesses in the security of a system. For example, TAMUK users must not run password cracking programs, packet sniffers, network mapping tools, or port scanners while connected in any manner to the TAMUK network infrastructure.
9. Users are not permitted to alter network hardware in any way.

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