Virus Procedure

Introduction
The number of computer security incidents and the resulting cost of business disruption and service restoration continue to escalate. Some actions that can be taken to reduce the risk and drive down the cost of security incidents are implementing solid security procedures, blocking unnecessary access to networks and computers, improving user security awareness, and early detection and mitigation of security incidents at Texas A&M University- Kingsville (TAMUK).

Purpose
The purpose of this procedure is to describe the requirements for dealing with computer virus, worm and Trojan Horse prevention, detection and cleanup.

Audience
This procedure applies to individuals that use any University Information Resources.

Virus Procedure
1. Any computer system connected to the University network must use iTech approved anti-virus software.
2. The anti-virus software must be in working order at all times and should never be disabled or bypassed.
3. The settings for the anti-virus software must not be altered in a manner that will reduce the effectiveness of the software.
4. The anti-virus software must be up to date with the most current patches and updates and virus definitions must not be older than one week.
5. The anti-virus software automatic update frequency should be set to update at least once per week.
6. The email gateway must utilize iTech approved email anti-virus software and must adhere to iTech rules for the setup and use of this software.
7. Any virus that is not automatically cleaned by the anti-virus software constitutes a security incident and must be reported to the Help Desk.

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