Virus Policy

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 policies, blocking unnecessary access to networks and computers, improving user security awareness, and early detection and mitigation of security incidents.

1. Purpose
The purpose of the Computer Virus Policy is to describe the requirements for dealing with computer virus, worm and Trojan Horse prevention, detection and cleanup.

2. Audience
The Texas A&M University-Kingsville Computer Virus Policy applies equally to all individuals that use any University Information Resources.

3. Virus Policy
   3.1. Any computer system connected to a Texas A&M University-Kingsville owned or managed network must use TAMUK CIS approved virus protection software.
   3.2. The virus protection software must be in working order at all times and should never be disabled or bypassed.
   3.3. The settings for the virus protection software must not be altered in a manner that will reduce the effectiveness of the software.
   3.4. The virus protection software must be up to date with the most current patches and updates and virus definitions must not be older than 1 week.
   3.5. The virus protection software automatic update frequency should be set to update at least once per week.
   3.6. All Texas A&M University-Kingsville owned workstations, laptops and servers whether connected to the Texas A&M University-Kingsville network, or standalone, must use the TAMUK CIS approved virus protection software and configuration.
   3.7. All Texas A&M University-Kingsville owned workstations, laptops and servers must have the McAfee ePO agent installed and working correctly. The McAfee ePO agent should be configured to request policy definitions from the approved CIS ePO server.
   3.8. Each E-mail gateway must utilize TAMUK CIS approved e-mail virus protection software and must adhere to the CIS rules for the setup and use of this software.
   3.9. Every virus that is not automatically cleaned by the virus protection software constitutes a security incident and must be reported to the Help Desk.

4. Disciplinary Actions
Violation of this policy 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 Texas A&M University-Kingsville Information Resources access privileges, civil, and criminal prosecution.