29.01.99.K1.220 Antivirus Standard

Effective: April 1st, 2004
Revised: April 23rd, 2013
Revised: May 7, 2019
Next Scheduled Review: May 2024

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 standard is to describe the requirements for dealing with computer viruses or malware prevention.

Audience

This standard applies to individuals that use any University information resource.

Antivirus Standard

1. Any computer system connected to the University network must use iTech approved antivirus software.
2. The antivirus software should never be disabled or bypassed.
3. The settings for the antivirus software must not be altered in a manner that will reduce the effectiveness of the software.
4. The antivirus software must be up to date with the most current patches, updates and virus definitions.
5. The email gateway must utilize iTech approved email antivirus.
6. Any virus that is not automatically cleaned by the antivirus software constitutes a security incident and must be reported to the Information Security Officer (ISO).

Disciplinary Actions

Violation of this standard 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. IRM Act, 2054.075(b)
8. The State of Texas Information Act
9. The State of Texas Penal Code, Chapters 33 and 33A
10. Texas Administrative Code, Chapter 202
11. Texas A&M University-Kingsville Acceptable Use Procedure 29.01.99.K1.010
12. 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