g. Installing iTech approved anti-virus software
h. Setting up encrypted remote access if needed

3. Vulnerability assessments will be performed in accordance with the Vulnerability Assessment Procedures.
    a. Network/operating system vulnerabilities identified as high or medium risk must be corrected within the specified timeframe.
4. Violations of this standard must be reported to the Information Security Officer.

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. Computer Fraud and Abuse Act of 1986
2. Computer Security Act of 1987
3. DIR Standards Review and Recommendations Publications
4. DIR Practices for Protecting Information Resource Assets
5. IRM Act, 2054.075(b)
6. The State of Texas Information Act
7. The State of Texas Penal Code, Chapters 33 and 33A
8. Texas Administrative Code, Chapter 202
9. Texas A&M University-Kingsville Acceptable Use Procedure 29.01.99.K1.010
10. 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