29.01.99.K1.235 Vulnerability Management Standard

Effective: April 1st, 2004
Revised: October 24th, 2012
Revised: May 7, 2019
Next Scheduled Review: May 2024

Introduction

Periodic system scans will be performed on all systems providing services to system users and hosts at Texas A&M University-Kingsville (TAMUK). Vulnerability scans are performed to identify risk, and proactively mitigate security weaknesses. When systems vulnerabilities and exploits are not remediated escalation procedures begin with reporting noncompliance to the Dean or Assistant Vice President and ending with termination of network access for the system.

Purpose

The purpose of this standard is to outline vulnerability management at TAMUK.

Audience

This standard applies to individuals that use TAMUK Information Resources

Vulnerability Management Standard

1. Awareness
   Monthly security scans will ensure that all servers are properly patched and secure. Any vulnerability found shall be reported to the system custodian and will require remediation/mitigation. This will help ensure data security, integrity and reliability
2. Remediation
   a. System custodians review the reports and remediate/mitigate any reported critical and severe vulnerabilities.
   b. System custodians will be required to keep a log of mitigation steps taken to address reported vulnerabilities every month.
3. Verification

a. Server is scanned in the next monthly cycle. If the same vulnerabilities exist, the system custodian and supervisor are notified that vulnerabilities must be remediated within the next 10 business days.
b. If the vulnerabilities still remain, the system will be removed from the network. A notification will be sent to the system custodian and supervisor of the removal.

Disciplinary Actions

Violation of this standard may result in disciplinary action up to and including termination for employees and temporaries; a termination of contractual 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 Practices for Protecting Information Resources (nd