1. **Overview**
   Periodic system scans will be performed on all systems providing services to system users and hosts. 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 VP and ending with termination of network access for the system.

2. **Awareness**
   Monthly security scans will ensure that all servers are properly patched and secure. Any vulnerability found shall be reported to the server custodian and will require remediation/mitigation. This will help ensure data security, integrity and reliability.

3. **Remediation**
   3.1. System custodians are to review the reports and remediate/mitigate any reported critical and severe vulnerabilities.
   3.2. System custodians will be required to keep a log of mitigation steps taken to address reported vulnerabilities every month.

4. **Non-compliance**
   Violations of this policy may result in shutting down ports, services and or disciplinary action. Repeated violations of this policy may include disciplinary actions 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.