Systems Development Policy

Introduction
The number of computer security incidents and the resulting cost of business disruption and service restoration continue to escalate. By implementing solid security policies, blocking unnecessary access to networks and computers, improving user security awareness, and early detection and mitigation of security incidents are some of the actions that can be taken to reduce the risk and drive down the cost of security incidents.

Purpose
The purpose of the System Development Policy is to describe the requirements for developing and/or implementing new software in the Texas A&M University-Kingsville Information Resources.

1. Audience
1.1. The Texas A&M University-Kingsville System Development Policy applies equally to all individuals that use any University Information Resources.

2. Systems Development Policy
2.1. Computing and Information Services (CIS) is responsible for developing, maintaining, and participating in a System Development Life Cycle (SDLC) for Texas A&M University-Kingsville system development projects. All software developed in-house which runs on production systems must be developed according to the SDLC. At a minimum, this plan should address the areas of preliminary analysis or feasibility study; risk identification and mitigation; systems analysis; general design; detail design; development; quality assurance and acceptance testing; implementation; and post-implementation maintenance and review. This methodology ensures that the software will be adequately documented and tested before it is used for critical Texas A&M University-Kingsville information.
2.2. All production systems must have designated Owners and Custodians for the critical information they process. CIS must perform annual risk assessments of production systems to determine whether the controls employed are adequate.
2.3. All production systems must have an access control system to restrict who can access the system as well as restrict the privileges available to these Users. A designated access control administrator (who is not a regular User on the system in question) must be assigned for all production systems.
2.4. Where resources permit, there should be a separation between the production, development, and test environments. This will ensure that security is rigorously maintained for the production system, while the development and test environments can maximize productivity with fewer security restrictions. Where these distinctions have been established, development and test staff must not be permitted to have access to production systems. Likewise, all production software testing must utilize sanitized information.
2.5. All application-program-based access paths other than the formal user access paths must be deleted or disabled before software is moved into production.
2.6. Violations of this policy must be reported to the Security Analyst or ISO.

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.