Physical Access Policy

Introduction
Technical support staff, security administrators, system administrators, and others may have Information Resource physical facility access requirements as part of their function. The granting, controlling, and monitoring of the physical access to Information Resources facilities is extremely important to an overall security program.

1. Purpose
   1.1. The purpose of the Texas A&M University-Kingsville Physical Access Policy is to establish the rules for the granting, control, monitoring, and removal of physical access to Information Resource facilities.

2. Audience
   2.1. The Texas A&M University-Kingsville Physical Access Policy applies to all individuals within the Texas A&M University-Kingsville enterprise that are responsible for the installation and support of Information Resources, individuals charged with Information Resources security, and data owners.

3. Physical Access Policy
   3.1. A risk assessment will be performed annually using the Information Security Awareness, Assessment, and Compliance utility from TAMU (ISAAC).
   3.2. All physical security systems must comply with all applicable regulations including, but not limited to, building codes and fire prevention codes.
   3.3. Physical access to all Information Resources restricted facilities must be documented and managed.
   3.4. All IR facilities must be physically protected in proportion to the criticality or importance of their function at Texas A&M University-Kingsville.
   3.5. Access to Information Resources facilities must be granted only to Texas A&M University-Kingsville support personnel, and contractors, whose job responsibilities require access to that facility.
   3.6. The process for granting card and/or key access to Information Resources facilities must include the approval of the person responsible for the facility and approval of the person responsible for the IR equipment.
   3.7. Each individual that is granted access rights to an Information Resources facility must receive emergency procedures training for the facility and must sign the appropriate access and non-disclosure agreements.
   3.8. Requests for access must come from the applicable Texas A&M University-Kingsville data/system owner.
   3.9. Access cards and/or keys must not be shared or loaned to others.
   3.10. Access cards and/or keys that are no longer required must be returned to the person responsible for the Information Resources facility. Cards must not be reallocated to another individual bypassing the return process.
   3.11. Lost or stolen access cards and/or keys must be reported to the person responsible for the Information Resources facility/equipment.
   3.12. Keys must not have identifying information other than a return mail address.
   3.13. All Information Resources facilities that allow access to visitors will track visitor access with a sign in/out log.
   3.14. A service charge may be assessed for access cards and/or keys that are lost, stolen or are not returned.
   3.15. Card access records and visitor logs for Information Resources facilities must be kept for routine review based upon the criticality of the Information Resources being protected.
   3.16. The person responsible for the Information Resources facility must remove the card and/or key access rights of individuals that change roles within Texas A&M University-Kingsville or are
3.17. Visitors must be escorted in access controlled areas of Information Resources facilities.
3.18. The person responsible for the Information Resources facility must review access records and visitor logs for the facility on a periodic basis and investigate any unusual access.
3.19. The person responsible for the Information Resources facility must review card and/or key access rights for the facility on a periodic basis and remove access for individuals that no longer require access.
3.20. Signage for restricted access rooms and locations must be practical, yet minimal discernible evidence of the importance of the location should be displayed.
3.21. All access records and reports are confidential and disclosure of those records or reports is a violation of this policy.

**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. Violations of this policy or any components of this policy must be reported to the CIO and Provost.