Physical Access Procedure

Introduction
Technical support staff, security administrators, system administrators, and others at Texas A&M University-Kingsville (TAMUK) 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.

Purpose
The purpose of this procedure is to establish the rules for the granting, control, monitoring, and removal of physical access to information resource facilities.

Audience
This procedure applies to individuals within the University that are responsible for the installation and support of information resources, individuals charged with information resources security, and data owners.

Physical Access Procedure
1. A risk assessment will be performed annually.
2. Physical access to facilities containing critical or sensitive information resources must be documented and managed.
3. Access to critical or sensitive information resources facilities must be granted only to University personnel and contractors, whose job responsibilities require access to that facility.
4. The process for granting card 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 information resource.
5. Access cards or keys must not be shared or loaned to others.
6. When physical access requirements change and access to information resource facility is no longer needed:
   a. Keys that are no longer required must be returned to Physical Plant.
   b. Card access will be deactivated for the facility.
7. Lost or stolen access cards or keys must be reported to the person responsible for the information resources facility.
8. Keys must not have identifying information other than a return mail address.
9. Visitors to information resources facilities must be accompanied by authorized personnel.
10. A service charge may be assessed for access cards or keys that are lost, stolen or are not returned.
11. The person responsible for the information resources facility must review card or key access rights for the facility on a periodic basis and remove access for individuals that no longer require access.
12. Access records and reports are confidential. Access to records and reports must be requested from the University Compliance Officer.
Disciplinary Actions
Violation of this procedure 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 TAMUK Information Resources access privileges, civil, and criminal prosecution.

References
1. Copyright Act of 1976
2. Computer Fraud and Abuse Act of 1986
4. DIR Practices for Protecting Information Resources Assets
5. DIR Standards Review and Recommendations Publications
7. The Health Insurance Portability and Accountability Act of 1996 (HIPAA)
8. IRM Act, 2054.075(b)
9. The State of Texas Information Act
10. The State of Texas Penal Code, Chapters 33 and 33A
11. Texas Administrative Code, Chapter 202
12. Texas A&M University-Kingsville Procedure 29.01.03.K1.010
13. Texas A&M University-Kingsville Procedure 29.01.04.K1.010
14. Texas Government Code, Section 441