29.01.99.K1.130

Physical Access Standard Administrative Procedure

Effective: April 1, 2004
Revised: April 26, 2013
Revised: March 13, 2019
Next Scheduled Review: March 13, 2024

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 confidential or sensitive information resources must be documented and managed.
3. Access to confidential or sensitive information resource facilities may be granted to University personnel, contractors and other authorized personnel whose job responsibilities require access to that facility.

4. The process for granting card or key access to information resource 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 an individual's 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 must be accompanied by authorized personnel when visiting information resource facilities.
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. Physical access records shall be maintained as appropriate for the criticality of the information resources being protected. 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 contract relations in the case of contractors or consultants; dismissal for interns and volunteers; or suspension or expulsion in the case of students. Additionally, individuals are subject to loss of TAMUK Information Resources access privileges, civil, and criminal prosecution.

References

1. DIR Practices for Protecting Information Resources Assets
2. The State of Texas Information Act
3. Texas Administrative Code, Chapter 202
4. Texas A&M University-Kingsville Acceptable Use Procedure 29.01.99.K1.010
5. Texas Administrative Code 202.75 Information Resources Security Safeguards
6. System Policy 29.01 Information Resources
7. System Regulation 29.01.03 Electronic Information Services Access and Security

Contact Office

For More Information, Contact: iTech
MSC 185, 700 University Blvd., Kingsville, TX 78363-8202
Contact Phone: 361-593-2404