PRAIRIE VIEW A&M UNIVERSITY
UNIVERSITY ADMINISTRATIVE PROCEDURE

29.01.03.P0.09 Information Resources – Physical Access
Approved May 26, 2009
Revised July 1, 2015
Revised June 3, 2020
Next Scheduled Review: June 2025

UAP Purpose

The purpose of this University Administrative Procedure (UAP) is to establish the process for the granting, control, monitoring, and removal of physical access to information resource facilities. In addition, the performance of these procedures is necessary to ensure compliance with the Texas Administrative Code Ch. 202, Subch. C, Information Security Standards for Higher Education.

Definitions

Confidential Information - information that is exempt from disclosure requirements under the provisions of applicable state or federal law, e.g., The Texas Public Information Act.

Information Resources (IR) - the procedures, equipment, and software that are designed, employed, operated, and maintained to collect, record, process, store, retrieve, display, and transmit information or data.

Mission Critical Information - information that is defined by the University or information resource owner to be essential to the continued performance of the mission of the University or department. Unavailability of such information would result in more than an inconvenience. An event causing the unavailability of mission critical information would result in consequences such as significant financial loss, institutional embarrassment, failure to comply with regulations or legal obligations, or closure of the University or department.

Information Resource Owner - an entity responsible for a business function and for determining controls and access to information resources supporting that business function.

Official Procedures and Responsibilities

1. GENERAL

1.1 Under the provisions of the Information Resources Management Act, information resources are strategic assets of the State of Texas that must be managed as valuable state resources. Technical support staff, 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 resource facilities is extremely important to an overall security program.

1.2 There may be additional measures that department heads or deans will implement to further mitigate risks. The assessment of potential risks and the application of appropriate mitigation measures are to be determined by the department heads and their identified information security administrators. In accordance with Texas Administrative Code Ch. 202, Subch. C, Information Security Standards for Institutions of Higher Education, each department and/or resource owner may elect not to implement some or all of the risk mitigation measures provided in this UAP based on documented information security risk management decisions and business functions. Such risk management decisions must be documented and approved by the designated Information Security Officer (ISO).

2. APPLICABILITY

2.1 This UAP applies to all University information resources. The intended audience for this UAP includes, but is not limited to, all information resources management personnel, owners, system administrators, and users of University information resources.

3. PROCEDURES

3.1 All physical security systems shall comply with applicable regulations such as, but not limited to, building codes and fire prevention codes.

3.2 Physical access procedures to all information resources facilities shall be documented and managed.

3.3 All information resource facilities shall be physically protected in proportion to the criticality or importance of their function at Prairie View A&M University.

3.4 Access to information resources facilities shall be granted only to departmental personnel, vendors, or other authorized personnel whose job responsibilities require access to that facility.

3.5 There shall be an approval and documentation process for granting and revocation/return of security codes, access cards, and/or key access to information resources facilities.

3.6 Individuals who are granted access rights to an information resource facility must sign appropriate access agreements. Facilities users should also receive information regarding appropriate physical security practices and emergency procedures.

3.7 Security access codes, access cards and/or keys to information resource facilities shall not be shared or loaned to others.

3.8 Appropriate departmental personnel responsible for the physical security of information resources shall review access rights for the facility on a periodic basis and revoke access for individuals that no longer require such access.

3.8.1 Access cards or keys must not be reallocated to another individual, bypassing the return process.

3.8.2 Access cards and/or keys must not have identifying information other than a return mail address.

3.9 Visitors must be escorted in restricted access areas of information resource facilities.

3.10 Physical access records shall be maintained as appropriate for the criticality of the information resources being protected. Such records shall be reviewed as needed by organizational unit heads or their designees.

Related Statutes, Policies, Regulations and Rules

Ch. 202, Subch. C, Information Security Standards for Institutions of Higher Education

Security Control Standards Catalog

Information Resources Management Act

System Policy 29.01 Information Resources

System Regulation 29.01.03 Electronic Information Services Access and Security

The Texas A&M University System Information Security Standards

Contact Office

Center for Information Technology Excellence	936-261-9350