

UNIVERSITY PROCEDURES
TEXAS A&M UNIVERSITY-CORPUS CHRISTI

21.01.06.C2.16 Physical Access

Approved June 11, 2007

Supplements University Rule 21.01.06.C2

1. GENERAL

Technical support staff, system administrators, and others at Texas A&M University-Corpus Christi 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. The purpose of the university physical access procedure is to establish the process for the granting, control, monitoring, and removal of physical access to information resource facilities.

2. APPLICABILITY

This university procedure applies to facilities that house multi-user systems (i.e., “data centers”) that process or store mission critical and/or confidential information.

The purpose of the implementation of this university procedure is to provide a set of measures that will mitigate information security risks associated with physical access. There may also be other or additional measures that will provide appropriate mitigation of the risks. The assessment of potential risks and the application of appropriate mitigation measures are to be determined by the information resource owner or their designee. In accordance with Texas Administrative Code 202 - Information Security Standards, each department and/or resource owner may elect not to implement some or all of the risk mitigation measures provided in this university procedure based on information security risk management decisions and business functions. Such risk management decisions must be documented in the annual security assessment report (See University Rule 21.01.06.C2 Security of Electronic Information Resources).

Responsibility for ensuring secure physical access to information resources may be part of the job function for departmental staff which may include, but not be limited to, information technology staff, system administrators, supervisors, managers, and others.

3. DEFINITIONS

Please refer to University Procedure 21.01.06.C2.01 Definitions.

4. PROCEDURES

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

UNIVERSITY PROCEDURES
TEXAS A&M UNIVERSITY-CORPUS CHRISTI

- 4.2. All information resource facilities must be physically protected in proportion to the criticality or importance of their function at the university and relative to the Sensitive Information maintained by the information resources.
- 4.3. Physical access to all restricted information resources facilities must be documented and managed.
- 4.4. Access to information resources facilities shall be granted only to university support personnel and contractors whose job responsibilities require access to that facility and shall be limited according to need and responsibilities as determined by the persons responsible for the information resource.
 - (1) 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 the persons responsible for the facility and the information resources.
 - (2) The persons responsible for the information resources facility must review all access rights for the facility on a periodic basis and remove access for individuals that no longer require access.
 - (3) Information pertaining to access to information resources must be retained according to Texas A&M System records retention guidelines.
- 4.5. The process for granting access to areas containing information resources must document the assigned privileges and include the approval of the persons responsible for the facility as well as the persons responsible for the information resources.
 - (1) Each individual that is granted access rights to an information resources facility must sign the appropriate access and non-disclosure agreements and shall receive emergency procedures training for the facility.
 - (2) Information pertaining to granting access to information resources must be retained according to Texas A&M System records retention guidelines.
 - (3) Security access cards, tokens, and/or keys issued by or for the university or any of its departments or organizations must not contain Sensitive Information pertaining to the individual, the information resource facility, or the university.
- 4.6. Security access codes, cards, tokens, and/or keys to information resource facilities shall not be shared or loaned to others. Should any of these items be lost or stolen, the incident shall be immediately reported to the persons responsible for issuing the access credentials.

UNIVERSITY PROCEDURES

TEXAS A&M UNIVERSITY-CORPUS CHRISTI

- 4.7. Visitors must be escorted in card access controlled areas of information resources facilities.
- 4.8. Security access cards, tokens, and/or keys that are no longer required must be returned to the person responsible for issuing the access credentials. These items must not be reallocated to another individual bypassing the return process.
- 4.9. Signage for restricted access to rooms and other locations must be practical, yet minimal discernible evidence of the importance of the location should be displayed.

5. CONSEQUENCES FOR VIOLATIONS

All university employees to include staff, tenured and non-tenured faculty, graduate assistants, student workers, interns, guests, volunteers, and probationary, temporary, or wage employees as well as contractors, consultants, and vendors required to adhere to this university procedure may be subject to criminal, civil, or disciplinary actions consistent with federal and state laws, system policies, and university rules.

Individuals found in violation of this university procedure are subject to loss of access privileges to university information resources (e.g. servers, workstations, email, etc). In addition, contracts associated with contractors, consultants, or vendors are subject to review and possible termination. Any device, system, or software found in violation of this procedure may be confiscated and temporarily stored by the Information Resources Manager or a representative of the office.

Additional guidance may be found, but is not limited to, the following policies and rules.

- Texas A&M System Policy
 - 01.03 Appointing Power and Terms and Conditions of Employment
 - 07.01 Ethics Policy, TAMUS Employees
 - 32.02 Discipline and Dismissal of Employees
 - 32.02.02 Discipline and Dismissal Procedure for Nonfaculty Employees
 - 33 Employment, Standards of Conduct
- Texas A&M University-Corpus Christi Rule
 - 12.01.99.C3 Faculty Dismissals, Administrative Leave, Non-Reappointments and Terminal Appointments
 - 13.02.99.C1 Student Disciplinary Proceedings

Contact for Interpretation: Assistant Vice President for Technology

Office of Responsibility: Executive Vice President, Finance & Administration