

UNIVERSITY PROCEDURES
TEXAS A&M UNIVERSITY-CORPUS CHRISTI

21.01.06.C2.13 Network Access

Approved June 11, 2007

Supplements University Rule 21.01.06.C2

1. GENERAL

The information resources network infrastructure is provided by Texas A&M University-Corpus Christi for tenants of university facilities. It is important that the network infrastructure, which includes media, active electronic equipment (i.e., multiplexers, hubs, routers, etc.) and supporting software, be able to meet current performance requirements while retaining the flexibility to allow emerging developments in high speed networking technology and enhanced user services. The purpose of the university network access procedures is to establish the process for the access to the network infrastructure.

2. APPLICABILITY

This university procedure applies to all university network information resources.

The purpose of the implementation of this university procedure is to provide a set of measures that will mitigate information security risks associated with network 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).

The intended audience for this university procedure includes all system administrators and users of university information resources.

3. DEFINITIONS

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

4. PROCEDURES

- 4.1. Users and resource custodians shall only use network addresses that have been assigned to the information resource for which they are responsible. The user or resource custodian of an information resource shall notify Media and Computer Services when it or its interface has been transferred, replaced, or decommissioned.

UNIVERSITY PROCEDURES

TEXAS A&M UNIVERSITY-CORPUS CHRISTI

- 4.2. Users may not alter network interfaces or devices in any way. Resource custodians may manipulate network interfaces and devices which they have been assigned specific responsibility to maintain.
- 4.3. Remote access to the university network is only authorized through resources provided by Media and Computer Services or approved by the Information Resources Manager.
 - (1) Any and all remote access to information resources containing sensitive or critical information must be approved by the Information Resources manager.
 - (2) Remote access by the university contractors or vendors must be approved by the Information Resources Manager and follow these procedures the procedures set forth in 21.01.06.C2.24 Vendor Access.
- 4.4. The university network may not be extended or re-transmitted by any device, system, or software over any medium (wired, wireless, telecommunications, etc) without advance notice and approval of the Information Resource Manager.
- 4.5. Non-university computers or devices connecting to the network provided by the university must conform to all university standards for information resources.

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

UNIVERSITY PROCEDURES
TEXAS A&M UNIVERSITY-CORPUS CHRISTI

- 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