

**UNIVERSITY PROCEDURES**  
**TEXAS A&M UNIVERSITY-CORPUS CHRISTI**

---

**21.01.06.C2.09 Information Resource Privacy**

*Approved June 11, 2007*

*Supplements University Rule 21.01.06.C2*

1. GENERAL

Privacy policies are mechanisms used to establish the responsibilities and limits for system administrators and users in providing privacy in university information resources. The university has the right to examine information on information resources, which are under the control or custody of the university. The general right to privacy is extended to the electronic environment to the extent possible.

However, there should be no expectation of privacy beyond that which is expressly provided by applicable privacy laws. Privacy is limited by the Texas Public Information Act, administrative review, computer system administration, and audits.

2. APPLICABILITY

This university procedure applies to electronic information created, sent, received, or stored on information resources owned, leased, administered, or otherwise under the custody and control of the university.

The purpose of the implementation of this university procedure is to provide a set of measures that will mitigate information security risks associated with information resource privacy. 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 audience is all users and administrators of university information resources.

3. DEFINITIONS

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

4. PROCEDURES

**UNIVERSITY PROCEDURES**  
**TEXAS A&M UNIVERSITY-CORPUS CHRISTI**

---

- 4.1. Web sites available to the general public from university information resources shall abide by and contain a link to the university's privacy statement located at <http://www.tamucc.edu/privacy.htm>.
- 4.2. Services, such as, but not limited to, web sites available from university information resources, must not contain, display, or transmit any sensitive information without appropriate security measures as determined by the Information Resource Manager.
- 4.3. In accordance with Texas Administrative Code Rule 202.75 Information Resources Security Safeguards the Information Resource Manager may authorize the logging, monitoring, review, and interruption of all information passing through or stored on university information resources to ensure compliance with applicable laws, policies, rules, and procedures or to monitor network performance and maintenance activities.
- 4.4. The Information Resource Manager may provide law enforcement personnel access to information transmitted through and stored on university information resources after the notification and written approval of the Executive Vice President of Finance & Administration and university legal council. Exceptions to this procedure may occur in instances related to federal and state laws.
- 4.5. Resource custodians may examine personal and business related files when necessary to maintain the business continuity of the information resource. Access to these files must adhere to the following criteria:
  - (1) notification of the file owner or the owner's immediate supervisor as permitted by time,
  - (2) examination of files must be limited to only those files that are necessary to accomplish the specific task, and
  - (3) alterations of files shall be avoided unless necessary to maintain business continuity.
- 4.6. Information contained on university information resources is considered private and must not be accessed or modified, pursuant to the exceptions provided in 4.3, 4.4, and 4.5, by individuals other than the documented owner of the information.
- 4.7. Any actual or potential weaknesses in the security of information resources or disclosure of Sensitive Information must be reported according to the procedures outlined in University Procedure 21.01.06.C2.08 Incident Management.
- 4.8. Unless otherwise provided for, individuals whose relationship with the university is terminated (e.g., student graduates; employee takes new job; visitors depart) are

## UNIVERSITY PROCEDURES

### TEXAS A&M UNIVERSITY-CORPUS CHRISTI

---

considered to cede ownership to the information resource custodian. Custodians should determine what information is to be retained and delete all other.

- 4.9. The university collects and processes many different types of data from third parties. Much of this data is Sensitive Information and shall be protected in accordance with all applicable laws, regulations, rules, and procedures.

#### 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