# 29.01.03.C2.02 Acceptable Use

*Approved June 11, 2007*
*Reviewed September 15, 2011*
*Reviewed February 21, 2013*
*Supplements University Rule 29.01.03.C2*

1. GENERAL

Under the provisions of the Texas Information Resources Management Act, information resources are strategic assets of the State of Texas that must be managed as valuable state resources. Texas A&M University-Corpus Christi has developed other Rules and Procedures that address acceptable use of information resources. The purpose of this University Procedure is to provide a useful summary of some of the more important responsibilities that apply to all users of University information resources. Other responsibilities are defined in other Rules and Procedures.

2. APPLICABILITY

This University Procedure applies to all University 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 acceptable use of university information resources. 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.

The intended audience for this Procedure is all users of University information resources, including students, faculty, staff, and third parties.

Please also see Procedure 29.01.03.C2.25 – "Exceptions to Risk Mitigation Measures."

3. DEFINITIONS

Please refer to University Procedure 29.01.03.C2.01 Definitions.

4. ACCEPTABLE USE

4.1. All users must report to the IRM or the Office of Information Security any weaknesses in the security of the University's information resources, or any incidents of possible misuse or violation of this or any other policy related to the security of the University's information resources.

4.2. Users must not attempt to access any University information resource or data for which they do not have authorization or explicit consent. With the sole exception

of the incidental uses described in Section 5 of this Procedure, users must use University information resources only for legitimate University-business-related or academic-research-related purposes.

4.3. Users must not access, edit, delete, copy, transmit, distribute, or otherwise use confidential or University-sensitive data for which they do not have 1) a legitimate University-business-related or academic-research-related purpose for the particular use and 2) explicit authorization from the University for the particular use. Furthermore, users must not delete data that is protected by e.g., document retention laws (e.g., System Regulation 61.99.01) or e-discovery requirements. Incidental use of confidential or University-sensitive data is prohibited. (See also Procedure 21.01.06.C2.28: Classification and Protection of Data; Encryption.)

4.4. Users must not share their credentials, i.e., University account(s), passwords, Personal Identification Numbers (PIN), Security Tokens (i.e. Smartcard), or similar information or devices used for identification and authorization purposes. Likewise, users must not use the credentials of another. (See also Procedure 29.01.03.C2.15: Password.)

4.5. With the exception of the limited purposes described in System Regulation 33.04.01, users must not be paid, or otherwise profit, from the use of any University information resources or from any output produced from such resources. Users must not promote any commercial activity using University information resources.

4.6. Users must respect copyright. Users must not make unauthorized copies of copyrighted software or other copyrighted materials such as music, films, and textbooks. The University complies with all legal requests for information and will not hesitate to report a user's use in response to a lawful request. (See also Procedure 29.01.03.C2.22: Software Licensing.)

4.7. Users must not purposely engage in activity that may: harass, threaten or abuse others; degrade the performance of University information resources; deprive an authorized user access to a University resource; obtain extra resources beyond those allocated; circumvent University information security measures.

4.8. Users must not download, install or run security programs or utilities (e.g., password cracking programs, packet sniffers, or port scanners) that reveal or exploit weaknesses in the security of a system without the explicit prior approval of the IRM or his or her designees. (See also Procedure 29.01.03.C2.20 Security Monitoring and Scanning.)

4.9. Users must not intentionally access, create, store or transmit material which University may deem to be offensive, indecent or obscene (other than in the course of academic research where this aspect of the research has the explicit

approval of the University official processes for dealing with academic ethical issues). (See also System Policy 33.04: Use of System Resources.)

4.10. Users must not otherwise engage in acts against the aims and purposes of the University as specified in its governing documents or in rules, regulations and procedures adopted from time to time.

5. INCIDENTAL USE

Incidental use only applies to those information resources and data to which the user has been explicitly authorized. Incidental use of University-sensitive or confidential information is not permitted. The following restrictions apply:

5.1. Incidental personal use of University information resources including electronic mail, internet access, fax machines, printers, and copiers, is restricted to University-approved users; it does not extend to family members or other acquaintances.

5.2. Incidental use must not result in more than nominal direct costs to the University.

5.3. Incidental use must not interfere with the normal performance of an employee's work duties.

5.4. Storage of personal email messages, voice messages, files, and documents within university information resources must be nominal.

5.5. All messages, files, and documents, including personal messages, files, and documents located on university information resources, may be subject to open records requests, and may be accessed in accordance with this procedure.

6. 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
  - 33.04.01 Use of System Resources for External Employment
- 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: Office of Information Security

Office of Responsibility: Office of the Associate VP for Information Technology and CIO