29.01.03.C2.07 Email and Other Electronic Communications Use

Approved June 11, 2007
Reviewed March 19, 2012
Supplements University Rule 29.01.03.C2

1. GENERAL

University information resources are strategic assets and as such must be managed as valuable state resources. Since a large portion of university business is conducted using emails, instant messaging, chat, or any other electronic communications. It is important that these services function in an efficient and reliable manner. These procedures, therefore, address expected standards for university emails, instant messaging, chat, or any other electronic communications.

2. APPLICABILITY

This university procedure applies to the use of emails, instant messaging, chat, or any other electronic communications stored on or passing through any university owned 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 emails, instant messaging, chat, or any other electronic communications. 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.

Please also refer to Procedure 29.01.03.C2.25 “Exceptions from Risk Mitigation Measures.”

The intended audience for this university procedure includes, but is not limited to any university employee, student, guest, or visitor that may use any university information resource that has the capacity to send, receive, or store emails, instant messaging, chat, or any other text based communications.

3. DEFINITIONS

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

4. PROCEDURES

4.1. All emails, instant messaging, chat, or any other electronic communications are required to adhere to:

UNIVERSITY PROCEDURES
TEXAS A&M UNIVERSITY-CORPUS CHRISTI
Faculty and staff who are not in compliance with the biannual ethics, diversity, and security training shall have their access to university emails, instant messaging, chat, and any other electronic communications suspended.

All emails, instant messaging, chat, or any other electronic communications that contain Sensitive Information must be encrypted during transmission and storage.

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 emails, instant messaging, chat, or any other electronic communications that are stored on or pass through university information resources to ensure compliance with applicable laws, policies, rules, and procedures or to monitor network performance and maintenance activities.

Before using portable computing devices for emails, instant messaging, chat, or any other text-based communications, the owner must ensure that the device adheres to University Procedure 29.01.03C2.17 Portable Computing.

For resource consolidation, business continuity, and security purposes all university emails, instant messaging, chat, and any other electronic communications transmission shall only be provided and maintained by Media and Computer Services.

The Information Resource Manager is responsible for development, documentation, and enforcement of university wide electronic communications standards such as, but not limited to, email quotas, backup and storage, email addresses, acceptable usernames, file transfers, etc.

All official university electronic communications to student, faculty, and staff must be sent to the faculty and staff domain (@tamucc.edu) or the student domain (@islander.tamucc.edu). The domain @tamucc.edu shall not be automatically forwarded from the university email server.
4.8. Electronic communications such as email and instant messaging/chat transcripts are subject to the same records retention rules that apply to other documents and must be retained in accordance with departmental records retention schedules.

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: Information Security Office

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