TARLETON STATE UNIVERSITY

A-Z Directory Maps Calendar Bookstore Giving

Division of Finance & Administration

Innovative Technology Solutions

MEET THE TEAM SECURITY SERVICES SUPPORT

Tarleton Office of Innovative Technology Solutions (OITS) Email Use Standard

Effective: February 11, 2020

Revised: April 25, 2025

Procedure Summary

Tarleton State University's (Tarleton or university) information resources are strategic assets which, as property of the State of Texas, must be managed as valuable state resources in accordance with **Texas Government Code Chapter 2054**. Since a large portion of Tarleton business is conducted using email, it is important that email services function in an efficient and reliable manner. This standard, therefore, addresses expected standards for university email usage.

This standard provides information regarding the use of email through university owned information resources. The purpose of the implementation of this standard is to provide a set of measures that will mitigate information security risks associated with email use. 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 (TAC) Chapter 202 -**

Español

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 standard based on information security risk management decisions and business functions. Such risk management decisions must be documented and reported to the designated information security officer.

This standard administrative procedure (SAP) applies to any Tarleton employee, third-party vendor, student, guest, or visitor that may use any university information resource that has the capacity to send, receive and/or store email.

Please see the Tarleton Security Controls Catalog, specifically the **Access Control (AC)**, **System and Communications Protection (SC)**, and **Assessment, Authorization, and Monitoring (CA)** families, for additional information and requirements.

Procedures and Responsibilities

1. The following activities are prohibited:
   - 1.1. Sending email that is intimidating or harassing;
   - 1.2. Using email for conducting personal business;
   - 1.3. Using email for purposes of political lobbying or campaigning;
   - 1.4. Violating copyright laws by inappropriately distributing protected works;
   - 1.5. Posing as anyone other than oneself when sending email, except when authorized to send messages for another user based on job duties or when serving in a support role; and
   - 1.6. The use of unauthorized email software.
2. The following activities are prohibited because they impede the functioning of network communications and the efficient operations of electronic mail systems:
   - 2.1. Sending or forwarding chain letters;
   - 2.2. Sending unsolicited messages to large groups except as required to conduct university business;
   - 2.3. Sending excessively large messages; and
   - 2.4. Sending or forwarding email that is likely to contain computer viruses.
3. All sensitive and/or confidential Tarleton material transmitted over an external network should be encrypted.
4. All user activity on Tarleton information resources and/or assets is subject to monitoring and review.
5. Electronic mail users must not give the impression that they are representing, giving opinions, or otherwise making statements on behalf of Tarleton or any unit of the university unless appropriately authorized (explicitly or implicitly) to do so. Where appropriate, an explicit disclaimer will be included unless it is clear

from the context that the author is not representing Tarleton. An example of a simple disclaimer is: “the opinions expressed are my own, and not necessarily those of my employer.”

6. Individuals must not send, forward or receive confidential or sensitive Tarleton information through non-Tarleton email accounts. Examples of non-Tarleton email accounts include, but are not limited to: Hotmail, Gmail, Yahoo mail, AOL mail, and email provided by other Internet Service Providers (ISP).
7. Auto-forwarding, including mailbox or smtp forwarding, shall not be used to send or forward any email from internal staff/faculty/student worker email accounts to non-Tarleton email accounts/domains. Any exceptions to this must be reviewed and approved by the Tarleton Information Security Officer (ISO)/Chief Information Security Officer (CISO).

Definitions

Confidential Information: information that is excepted from disclosure requirements under the provisions of applicable state or federal law, e.g. the Texas Public Information Act.

Information Resources (IR): the standards, equipment, and software that are designed, employed, operated, and maintained to collect, record, process, store, retrieve, display, and transmit information or data.

Information Security Officer (ISO) / Chief Information Security Officer (CISO): responsible for administering the information security functions within the university and reports to the information resources manager (IRM).

Related Statutes, Policies, or Requirements

TAMUS Policy 29.01, Information Resources

TAMUS Regulation 29.01.02, Use of Licensed Software

TAMUS Regulation 29.01.03, Information Security

TAMUS Regulation 29.01.04, Accessibility of Electronic and Information Resources

TAMUS Regulation 29.01.05, Artificial Intelligence

TAMUS Regulation 29.01.06, Covered Applications and Prohibited Technologies

Tarleton SAP 29.01.03.T0.01, Information Resources – Acceptable Use

Tarleton Rule 29.01.99.T1, Information Resources

Tarleton Security Controls Catalog

Contact Office

Office of Innovative Technology Solutions

AVP and CIO of Innovative Technology Solutions

254-459-5685

TARLETON STATE UNIVERSITY

125 YEARS OF EXCELLENCE

Contact Tarleton State

1333 W. Washington
Stephenville, TX 76402

254-968-9000

Resources

Compact with Texans
Disability Accommodations
Mental Health Resources
Rules, Notices & Public Info

Transparency & Reporting

Accreditation
Campus Carry
Campus Safety

Clery Act

Equal Opportunity

Course Schedules, Syllabi & Faculty CVs

Open Records

Risk, Fraud & Misconduct Hotline

Sexual Misconduct Policies

State Resources

State of Texas

Texas CREWS

Texas Homeland Security

Texas Veterans Portal

MEMBER OF THE
TEXAS A&M
UNIVERSITY
SYSTEM

Site Policies

Accessibility

Sitemap

Report a Website Problem