29.01.03.H0.26 Multi-Factor Authentication Standard Administrative Procedure

Approved: February 1, 2029
Next Scheduled Review: February 2029

Procedure Summary

Confidential and sensitive information hold significant value as information assets for Texas A&M University – Texarkana (TAMUT). Consequently, an additional cybersecurity protocol and service will be implemented to safeguard such information through the adoption of Multi-Factor Authentication (MFA). This measure will guarantee that only authorized personnel possess access to confidential or sensitive data.

This procedure pertains to all faculty and staff who access systems containing confidential or sensitive information. It is the responsibility of the individual possessing or directly controlling such information to ascertain that suitable risk mitigation strategies are implemented to avert unauthorized data exposure.

Procedures and Responsibilities

General Information

1. Information Technology (IT) will use Microsoft MFA as the standard Multi-Factor Authentication (MFA).
    a. The default authentication method is to use the free Microsoft Authenticator app. If end users have it installed on their mobile device.
    b. Alternatively, end users can use SMS messages sent to their phone.
    c. “Remember me” must not exceed 5 days.
2. Information owners and custodians will notify IT of any information resource that contains confidential or sensitive information.
    a. Information resources identified must be protected with MFA.
        i. The information resource vendor must integrate with Microsoft MFA; or,
        ii. As SSO requires MFA, systems that are only accessible through VPN or Office 365 applications are also protected.
    b. Exceptions may be requested through opening up a ticket with IT asking for an exception with a justification for ITAC to review the request, approve or deny the request, and/or approve the request yearly.

Disciplinary Actions

Noncompliance with this procedure may result in disciplinary measures up to and including termination of employment or temporary status for employees, contract termination for contractors or consultants, dismissal for interns and volunteers, or suspension or expulsion for students. Moreover, individuals may be subjected to the revocation of their access privileges to TAMUT Information Resources, as well as civil and criminal prosecution.

Related Statutes, Policies, or Requirements

Texas Administrative Code, Chapter 202
University Procedure 29.01.99.H0.02, *Acceptable Use*
System Regulation 29.01.03, *Information Security*

Contact Office

Office of Information Technology
903-334-6603