29.01.99.K1.XXX

Multi-Factor Authentication Standard Administrative Procedure

Approved: February 13, 2019
Next Scheduled Review: February 13, 2024

Introduction

Confidential and sensitive information are important information assets to the University. As such, an additional cybersecurity protocol and service to protect this kind of information will be provided through the use of Multi-Factor Authentication (MFA). This will ensure that only appropriate individuals have access to confidential or sensitive information.

Purpose

The purpose of this procedure is to provide guidance on the implementation of multi-factor authentication at TAMUK to protect confidential or sensitive information.

Audience

This procedure applies to all individuals accessing systems with confidential or sensitive information. It is the responsibility of the individual having confidential or sensitive information in their possession or under their direct control to ensure that appropriate risk mitigation measures are in place to protect data from unauthorized exposure.

Multi-Factor Authentication Procedure

1.) iTech will use Duo as the standard Multi-Factor Authentication (MFA).
    a. "Remember me" must not exceed 60 days.
2.) Information owners and custodians will notify iTech of any information resource that contains confidential or sensitive information by September 1, 2019.
    a. Information resources identified must be protected with MFA.
        i. The information resource vendor must integrate with Duo; or,
        ii. As JNet or SSO requires MFA, systems that are only accessible through JNet or SSO are also protected.
    b. Exceptions may be requested through the iTech Standard Administration Procedure 29.01.99.K1.005.

Disciplinary Actions

Violation of this procedure may result in disciplinary action up to and including termination for employees and temporaries; a termination of contract relations in the case of contractors or consultants; dismissal for interns and volunteers; or suspension or expulsion in the case of students. Additionally, individuals are subject to loss of TAMUK Information Resources access privileges, civil, and criminal prosecution.

References

1. DIR Practices for Protecting Information Resources Assets
2. DIR Standards Review and Recommendations Publications
3. The State of Texas Information Act
4. Texas Administrative Code, Chapter 202
5. Texas A&M University-Kingsville Acceptable Use Procedure 29.01.99.K1.010
6. Texas Government Code, Section 441
7. TAMU System Policy 29.01.03 Information Security

Contact Office

For More Information, Contact: iTech
MSC 185, 700 University Blvd., Kingsville, TX 78363-8202
Contact Phone: 361-593-2404