Multi-Factor Authentication Standard

1. Purpose

This standard establishes the minimum requirements aligned with current security best practices and developed in response to UTS-165 4.7, to ensure the confidentiality and integrity of UTRGV confidential data. Adherence to this standard enhances the protection of University information resources against unauthorized access by providing an additional layer of security. These minimum requirements complement all other UTRGV policies as well as applicable federal and state regulations governing the protection of UTRGV's data.

2. Scope

Ensuring that only authorized users access sensitive information by implementing multifactor authentication, which verifies user identity through multiple forms of evidence.

3. Audience

All faculty, staff, student employees, retirees, ex-employees, contractors, and vendors that are accessing, viewing, or editing confidential data or other critical university resources.

4. Authority

UTS 165

5. Definitions

MFA: Multi-Factor authentication or MFA, sometimes referred to as two-factor authentication or 2FA, is a security enhancement that allows you to present two pieces of evidence – your credentials – when logging in to an account. Your credentials fall into any of these three categories: something you know (like a password or PIN), something you have (like a smart card), or something you are (like your fingerprint).

Remote Access: Access to University Information Resources that originates from a Remote Location.

Remote Location: A location outside the physical UTRGV network boundary of the Institution (inclusive of University leased/rented properties and locations within the University's compliance environment).

6. Standard Details

MFA is required in the following situations:

a) When an employee or other individual providing services on behalf of the University (such as a student employee, contractor, or volunteer) logs on to a University network using an enterprise Remote Access gateway such as VPN, Terminal Server, Connect, Citrix, or similar services;

b) When, remotely accessing an online function such as a web page to view or modify employee banking, tax, or financial Information; or

c) When a Server administrator or other individual uses administrator credentials to access a Server that contains or has access to confidential university data; or

d) When, an individual described in a) is remotely accessing a web-based interface to University email; or an application that houses confidential university data, as defined by the UTRGV Data Classification Standard. Effective 7/31/2021

7. Exemptions and Non-Compliance

Exemptions have to be requested and submitted to the Information Security Office. Non-compliance with these standards may result in revocation of system or network access, notification of supervisors, and reporting to the Office of Internal Audit or Compliance.

University of Texas Rio Grande Valley employees are required to comply with both institutional rules and regulations and applicable UT System rules and regulations. In addition to university and System rules and regulations, University of Texas Rio Grande Valley employees are required to comply with state laws and regulations.

8. Related Policies, Standards, and Guidelines

- UT System (UTS 165) Information Resources Use and Security Policy
- UTS165 Standard 4: Access Management
- Data Classification Standard
- Center for Internet Security: Two-Factor Authentication Newsletter
- NIST Back to basics: Multi-factor authentication (MFA)