Two-Factor Authentication Standard

1. Purpose

This standard was created to set minimum requirements, which adhere to current security best practices and drafted in response to UTS-165 4.7, necessary to ensure the confidentiality and integrity of UTRGV confidential data. Compliance with this standard will add an extra layer of security in protecting University information resources from unauthorized access. These minimum requirements exist in addition to all other UTRGV policies and federal and state regulations governing the protection of UTRGV's data.

2. Scope

Assurance that only authorized users can gain access to critical information, by implementing two-factor authentication in order to verify the user identity using several types 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

Term	Description
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

2FA 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)

9. Revision History

Version	Date	New
1.0	4/4/2018	Created document
2.0	5/25/2018	Changes in sections: 3, 5, 6 and added 10
3.0	11/9/2018	Changes in section: 6 Letter e) Based on new UTS Mandate
4.0	3/28/2020	Section 6.d. Changed effective date of 2FA implementation for stated systems to July 31st 2021.

10. Approval History

Approval History			
Version	Date	Title	Name
2.0	6/5/2018	Chief Information Security Officer	Thomas Owen