INFORMATION RESOURCES ACCEPTABLE USE AND SECURITY POLICY AGREEMENT

All individuals granted access to or use of UTRGV or UT-System Information Resources must be aware of and agree toabide by the following acceptable use requirements:

A. Definitions

UTRGV: The University of Texas Rio Grande Valley
UT-System: The University of Texas System.
UTRGV Information Resources: All computer and telecommunications equipment, software, data, and media, owned or controlled by UTRGV or maintained on its behalf.
UTRGV Data: All data or information held on behalf of UTRGV, created as a result and/or in support of UTRGV business, or residing on UTRGV Information Resources,including paper records.
Confidential Data or Confidential Information: All UTRGV Data that is required to be maintained as private or confidential by applicable law(s).
User: Any individual granted access to UTRGV Information Resources.

B. General

1. UTRGV Information Resources are provided for the purpose of conducting the business of UTRGV and/or UT-System. However, Users are permitted to use UTRGV Information Resources that are incidental to the User's official UTRGV or UT-System duties (Incidental Use) as permitted by this policy.

2. Users have no expectation of privacy regarding any UTRGV Data residing on UTRGV owned computers, servers, or other information resources owned by, or held on behalf of, UTRGV. Additionally, users must also understand and accept that they have no expectation of privacy in any personal information stored by a User on a UTRGV or UT-System Information Resource, including UTRGV email accounts. UTRGV may access and monitor its Information Resources for any purpose consistent with the UTRGV's responsibilities, duties, and/or mission without notice.

3. Users have no expectation of privacy regarding any UTRGV Data residing on personally owned devices, regardless of why the Data was placed on the personal device.

4. All Users must comply with applicable UTRGV and UT-System Information Resources Use and Security policies, procedures, and standards at all times.
5. Users shall never use UTRGV Information Resources to deprive access to individuals otherwise entitled to access UTRGV Information Resources, to circumvent UTRGV computer security measures; or, in any way that is contrary to the UTRGV's mission(s) or applicable law(s).

6. Use of UTRGV Information Resources to intentionally access, create, store, or transmit sexually explicit materials is prohibited unless such use is required as part of the User's official duties as an employee of UTRGV and is approved in writing by the President or a specific designee. The viewing, access to, storage, or transmission of sexually explicit materials as Incidental Use is prohibited.

7. Users must clearly convey that the contents of any email messages or social media posts that are the result of Incidental Use are not provided on behalf of UTRGV and do not express the opinion or position of the UTRGV. An example of an adequate disclaimer is: "The opinions expressed are my own, and not necessarily those of my employer, The University of Texas Rio Grande Valley."

8. Users should report misuse of UTRGV Information Resources or violations of this policyto their supervisors or through an approved reporting format.

C. Confidentiality & Security of Data

1. Users shall access UTRGV Data only to conduct UTRGV business and only as permitted by applicable confidentiality and privacy laws. Users must not attempt to access data on systems they are not expressly authorized to access. Users shall maintain all records containing UTRGV data in accordance with the UTRGV information and data security policies, procedures, and standards, as well as the Records Retention Policy and Records Management Guidelines.

2. Users shall not disclose Confidential Data except as permitted or required by law and only aspart of their official UTRGV duties.

3. Whenever feasible, Users shall store Confidential Information or other information essential to the mission of UTRGV on a centrally managed server or UTRGV approved storage location, rather than a local hard drive or portable device.

4. In cases when a User must create or store Confidential or essential UTRGV Data on a local hard drive or a portable device, such as a laptop computer, tablet computer, or smartphone, the User must ensure the data is encrypted and secured in accordance with UTRGV, UT-System, and any other applicable requirements.
5. The following UTRGV Data must be encrypted during transmission over an unsecurednetwork: Social Security Numbers; personally identifiable Medical and Medical Payment information; Driver's License Numbers and other government-issued identification numbers;Education Records subject to the Family Educational Rights & Privacy Act (FERPA); creditcard or debit card numbers, plus any required code or PIN that would permit access to an individual's financial accounts; bank routing numbers; and other UTRGV Data about an individual likely to expose the individual to identity theft. Emails sent to and received from UT-System and UT-System institutions using UTRGV and/or UT-System provided email accounts are automatically encrypted. The Office of Information Technology [or other applicable offices] will provide tools and processes for Users to send encrypted data over unsecured networks to and from other locations.

6. Users who store UTRGV Data using Cloud services must use services provided by or sanctioned and approved by UTRGV through the approved UTRGV purchase process, rather than personally obtained Cloud services.

7. Users must not use security programs or utilities, except as such programs are required to perform their official duties on behalf of UTRGV. The use of security programs or utilities must be approved, in writing, by the UTRGV Chief Information Security Officer.

8. To help ensure the proper security of UTRGV Resources, all computers or other electronic devices connecting to a UTRGV network must run up-to-date operating systems, patches, and security software as prescribed by the Information Security Office.

9. Devices determined by the UTRGV to lack the required security standards, software, or to otherwise pose a threat to UTRGV Information Resources may be immediately disconnected by the UTRGV from a UTRGV network without notice.

D. Email

1. Emails sent or received by Users while conducting UTRGV business are UTRGV Data that is subject to state records retention and security requirements.

2. Users are to use UTRGV provided email accounts, rather than personal email accounts, for conducting UTRGV business.

3. The following email activities are prohibited when using a UTRGV provided email account:
    a. Sending an email under another individual's name or email address, except when authorized to do so by the owner of the email account for a work-related purpose.
    b. Accessing the content of another User's email account except 1) as part of an authorized investigation; 2) as part of an approved monitoring process; or 3) for other purposes specifically associated with the User's official duties on behalf of UTRGV.
    c. Sending or forwarding any email that is suspected by the User to contain computer viruses or malware.
    d. Any Incidental Use prohibited by this policy.
    e. Any use prohibited by applicable UTRGV or UT-System policy.

E. Incidental Use of UTRGV Information Resources

1. Incidental Use of UTRGV Information Resources must not interfere with the User's performance of official UTRGV business, result in direct costs to UTRGV, expose UTRGV to unnecessary risks, or violate applicable laws or other UTRGV or UT-System policy.

2. Users must understand that they have no expectation of privacy in any personal information stored by a User on a UTRGV or UT-System Information Resources, including UTRGV email accounts.

3. A User's incidental personal use of UTRGV Information Resources does not extend to the User's family members or others regardless of where the UTRGV Information Resource is physically located.

4. Incidental Use to conduct or promote the User's outside employment, including self-employment, is prohibited.

5. Incidental Use for purposes of political lobbying or campaigning is prohibited.

6. Storage of any email messages, voice messages, files, or documents created as Incidental Use by a User must be nominal (less than 5% of a User's allocated mailbox space).

7. Files not related to UTRGV or UT-System business may not be stored on network file servers.

F. Additional Requirements for Portable and Remote Computing

1. All electronic devices including personal computers, smartphones, or other devices used to access, create or store UTRGV Information Resources, including email, must be password protected in accordance with UTRGV requirements, and passwords must be changed whenever there is suspicion that the password has been compromised.
2. UTRGV Data created or stored on a User's personal computers, smartphones, other devices, or in databases that are not part of UTRGV's Information Resources are subject to Public Information Requests, subpoenas, court orders, litigation holds, discovery requests, and other requirements applicable to UTRGV Information Resources.

3. UTRGV-issued mobile computing devices must be encrypted and follow all UTRGV and UT-System device and security policies, procedures, and standards.

4. Any personally owned computing devices on which Confidential UTRGV Data is stored or created must be encrypted and follow all prescribed UTRGV and UT-System policies, procedures, and standards.

5. UTRGV Data created and/or stored on personal computers, other devices, and/or non-UTRGV databases should be transferred to UTRGV Information Resources as soon as feasible.

6. Unattended portable computers, smartphones, and other computing devices must be physically secured.

7. All remote access to networks owned or managed by the UTRGV or UT-System must be accomplished using a remote access method approved by UTRGV or UT-System, as applicable.

G. Password Management

1. UTRGV issued or required passwords, including digital certificate passwords, Personal Identification Numbers (PIN), Digital Certificates, Security Tokens (i.e., Smartcard), or similar information or devices used for identification and authorization purposes shall be maintained securely and shall not be shared or disclosed to anyone.

2. Each User is responsible for all activities conducted using the User's password or other credentials.

User Acknowledgment

Signature:_____ Date_____

Print Name:_____

Version Control – Acceptable Use Policy		
Activity	Date	Next Review
Version 1	2016	
Version 2	4/25/2022	Spring 2023