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 to abide 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, regardless of where that data or information is stored, and all information 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.

Prohibited Technology: Prohibited technology refers to any software, hardware, or other technological resources that are not allowed to be used within the University. This includes, but is not limited to, unauthorized security programs or utilities, and any technology that circumvents UTRGV computer security measures or is contrary to UTRGV's mission or applicable laws.

Artificial Intelligence (AI): A branch of computer science that involves the creation of systems capable of performing tasks that typically require human intelligence. Artificial Intelligence (AI) refers to the simulation of human intelligence processes by machines, especially computer systems. These processes include learning (the acquisition of information and rules for using the information), reasoning (using rules to reach approximate or definite conclusions), problem-solving, self-correction, and understanding natural language. AI applications can include expert systems, natural language processing (NLP), speech recognition, and machine vision.

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 UTRGV's responsibilities, duties, and/or mission without notice or permission from the user.

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 the 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. At a minimum, 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 UTRGV. An example of an adequate disclaimer is: "The opinions expressed are my own, and not necessarily those of The University of Texas Rio Grande Valley." Please consult University Marketing and Communications for further guidance and clarification.

8. Users should report misuse of UTRGV Information Resources or violations of this policy to 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.
2. Users must not attempt to access data on systems they are not expressly authorized to access.
3. Users shall maintain all records containing UTRGV data in accordance with:
    a. The UTRGV information and data security policies, procedures, and standards
    b. The UTRGV Records Retention Policy
    c. The Records Management Guidelines

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

5. 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.

6. 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.

7. The following UTRGV Data must be encrypted during transmission over an unsecured network:

    - 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)
    - Credit card or debit card numbers, plus any required code or PIN that would permit access to an individual's financial accounts
    - Bank routing numbers
    - 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 will provide tools and processes for Users to send encrypted data over unsecured networks to and from other locations.

8. 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 or the approved UTRGV authorization process, rather than personally obtained Cloud services.

9. 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.

10. 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.

11. 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 UTRGV from a UTRGV network without notice. Any exception must follow the UTRGV Information Security Office Security Exception Process.

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. Knowingly sending or forwarding any email that is suspected by the User to contain computer viruses, malware, or any other potentially harmful materials.
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 the use of Personal Portable Computing (BYOD)

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. Often these devices are referred to as Bring Your Own Device (BYOD).
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. Acceptable Use Guidelines for Remote Workers

1. Remote work offers flexibility and convenience, but it also requires adherence to specific additional guidelines to ensure the security and integrity of UTRGV Information Resources. The following additional guidelines outline the acceptable use of UTRGV Information Resources for remote workers:
    a. **Security Measures:**
        i. All electronic devices used to access, create, or store UTRGV

Information Resources must be password protected in accordance with UTRGV requirements. Passwords must be changed whenever there is suspicion that the password has been compromised.

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

iii 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.

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

b **Data Management:**

i 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.

ii 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.

c **Remote Access:**

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

d **Incident Reporting:**

iv Users should report any security incidents to the information security office at is@utrgv.edu or policy violations to their supervisors or through an approved reporting format.

e **Compliance:**

v Users must adhere to UTRGV and UT-System Information Resources policies, procedures, and standards at all times. This includes, but is not limited to, Prohibited Technology requirements, HIPAA requirements, AI requirements, International Travel requirements, and all other standards.

H. Acceptable Use Requirements for International Travel

1. When traveling internationally, it is essential to adhere to specific guidelines to ensure the security and integrity of UTRGV Information Resources. The following requirements outline the acceptable use of UTRGV Information Resources during international travel to non-adversary countries:
    a **Pre-Travel Preparation:**
        i Get the appropriate permissions and clearances.
            1 International Oversight Committee
            2 Export Control
            3 Information Security
            4 Information Technology
            5 Other approvals as required
        ii Ensure all electronic devices, including laptops, smartphones, and tablets, are encrypted and password-protected in accordance with UTRGV requirements.
        iii Update all operating systems, security patches, and antivirus software before departure.
        iv Back up all essential data to secure UTRGV-approved storage location before traveling.
        v If you are planning to travel to a designated adversary country, also known as a country of concern, you cannot travel with any UTRGV Information Resources and cannot have access to any UTRGV Information Resources.

        Please consult with the Office of Research Integrity and Export Compliance for information on current designated countries of concern.
    b **Data Management:**
        i Avoid storing sensitive or confidential UTRGV Data on personal devices. Use UTRGV-approved cloud services for data storage and access.
        ii Ensure that any UTRGV Data created or stored on personal devices is transferred to UTRGV Information Resources as soon as feasible.
    c **Remote Access:**
        i Use only UTRGV-approved remote access methods to connect to UTRGV networks while abroad.
        ii Avoid using public Wi-Fi networks for accessing UTRGV Information Resources. Use a secure VPN connection provided by UTRGV.
        iii While traveling in a adversary country (country of concern) access to UTRGV systems will be suspended because you are not allowed

to access UTRGV systems while in a adversary country (country of concern).

d **Incident Reporting:**
   i Report any security incidents or policy violations immediately to the Information Security Office or through an approved reporting format.

2. **Special Requirements for Travel to Adversary Countries, also known as Countries of Concern:** Travel to certain countries poses additional risks to the security of UTRGV Information Resources. Travel to adversary countries (also known as countries of concern) for business purposes is prohibited and travel for personal purposes to an adversary country (country of concern) requires prior notification and a post-travel debriefing. The following special requirements apply to travel to countries of concern:

   a **Pre-Travel Briefing & Training:**
      i After notification of personal travel has been made, you must obtain a pre-travel briefing from the appropriate offices to understand the specific risks and requirements associated with the destination country. Complete international travel training as required, including Information Security Office International Training.
   b **Device & Access Restrictions:**
      i You are not allowed to take UTRGV Information Resources or access UTRGV systems or data while in an adversary country (country of concern).
      ii Accessing UTRGV Data, including email from a country of concern is considered "a business purpose" and as such access is prohibited. This means while traveling to a country of concern you are not allowed to access any UTRGV system, including email, the LMS, or the Human Capital Management system (Oracle).
      iii Do not take taking devices or storage media that contain sensitive or confidential UTRGV Data. Taking such devices or storage media is considered a "business purpose" and is prohibited.

c **Post-Travel Actions:**

i Conduct a thorough security check of your personal devices upon return. Do not connect your personal devices to UTRGV resources until you have checked to ensure they were not compromised while you were traveling. Report any suspicious activity or potential security breaches to the Information Security Office immediately. Contact the International Oversight Committee to provide a post-travel debriefing.

I. Password Management

1. All electronic devices used to access, create, or store UTRGV Information Resources must be password protected in accordance with UTRGV requirements. Passwords must be changed whenever there is suspicion that the password has been compromised.

2. 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.

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

J. Prohibited Technologies Ban

1. Prohibited technology refers to any software, hardware, or other technological resources that are not allowed to be used within the University. This includes, but is not limited to, unauthorized security programs or utilities, and any technology that circumvents UTRGV computer security measures or is contrary to UTRGV's mission or applicable laws.

2. The use of prohibited technologies is strictly banned within the University to ensure the security and integrity of UTRGV Information Resources. 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.

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

4. See the Prohibited Technology Policy for additional information.

K. Appropriate and Permissible Uses of Artificial Intelligence

1. Artificial Intelligence (AI) should be used in a manner that aligns with the University's policies, ethical guidelines, and legal requirements. The appropriate use of AI involves utilizing AI technologies to enhance productivity, improve decision-making, and support the University's goals while ensuring data privacy, security, and compliance with relevant regulations. Users must ensure that AI applications do not compromise the confidentiality, integrity, or availability of UTRGV Information Resources.

   Permissible uses of AI include:

   a. Automating repetitive tasks to increase efficiency.
   b. Analyzing large datasets to extract valuable insights.
   c. Enhancing customer service through AI-powered chatbots.
   d. Supporting decision-making processes with predictive analytics.
   e. Improving cybersecurity measures by detecting and responding to threats in real-time.
   f. Approved activities supporting the academic, research, and medical missions of UTRGV.

2. It is important to use AI responsibly and ethically, ensuring that AI applications are transparent, fair, and do not discriminate against any individuals or groups. Users must also be aware of the potential risks associated with AI and take appropriate measures to mitigate them.

   At a minimum the ethical use of AI must provide for:

   - **Respect for Human Rights**: AI technologies should be used in ways that respect

and protect human rights, including privacy, dignity, and equality. Illegal or unethical use of AI technologies may result in disciplinary actions.

- **Transparency and Accountability:** Transparency in the development, use, or application of AI or AI enabled systems, platforms, or services, including disclosure of data sources, algorithms, and decision-making processes must be respected. Individuals must also be accountable for the outcomes and consequences related to the development or use of AI systems.
- **Bias Mitigation:** Where appropriate, users must actively work to identify, report, and mitigate biases in AI algorithms and data, and strive to create or utilize AI systems that are fair and objective.
- **Informed Consent:** When collecting and using data from humans, clear and understandable informed consent must be obtained from the data subject and adherence to all applicable legal and ethical standards must be maintained.

Further guidance on the use of AI can be found in the university's AI Policy and in additional Information Security Office requirements and in divisional specific guidelines.

L. Technology Assessment

All technology, including software, hardware, appliances, cloud and local services, and any tools for processing, storing, or transmitting data must be assessed and approved by the appropriate offices before purchase or installation on UTRGV Information Resources. This applies to open source, free, paid software, browser plugins/extensions, and all applications or services.

If you have any questions regarding this policy, please contact the Information Security Office at: is@utrgv.edu or by phone at 956-665-7823.

User Acknowledgment

Signature: _____ Date: _____

Print Name: _____