Acceptable Use Policy

Definitions:

- UTPB Information Resources: All computer and telecommunications equipment, software, data, and media, owned or controlled by UTPB or maintained on its behalf.
- UTPB Data: All data or information held on behalf of UTPB, created as result and/or in support of UTPB business, or residing on UTPB Information Resources, including paper records.
- Confidential Data or Confidential Information: All UTPB Data that is required to be maintained as private or confidential by applicable law.
- User: Any individual granted access to UTPB Information Resources.

General

- UTPB Information Resources are provided for the purpose of conducting the business of UTPB. However, Users are permitted to use UTPB Information Resources for use that is incidental to the User's official duties to UTPB (Incidental Use) as permitted by this policy.
- Users have no expectation of privacy regarding any UTPB Data residing on UTPB computers, servers, or other information resources owned by, or held on behalf, of UTPB. UTPB may access and monitor its Information Resources for any purpose consistent with UTPB's duties and/or mission without notice.
- Users have no expectation of privacy regarding any UTPB Data residing on personally owned devices, regardless of why the Data was placed on the personal device.
- All Users must comply with applicable UTPB Information Resources Use and Security policies at all times.
- Users shall never use UTPB Information Resources to deprive access to individuals otherwise entitled to access UTPB Information, to circumvent UTPB computer security measures; or, in any way that is contrary to UTPB's mission(s) or applicable law.
- Use of UTPB 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 UTPB and is approved in writing by the Chancellor or a specific designee. Viewing, access to, or storage or transmission of sexually explicit materials as Incidental Use is prohibited.
- 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 UTPB and do not express the opinion or position of UTPB. An example of an adequate disclaimer is: "The opinions expressed are my own, and not necessarily those of my employer, The University of Texas Permian Basin."
- Users should report misuse of UTPB Information Resources or violations of this policy to their supervisors.

Confidentiality & Security of Data

- Users shall access UTPB Data only to conduct UTPB 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 UTPB data in accordance with UTPB's Records Retention Policy and Records Management Guidelines.
- Users shall not disclose Confidential Data except as permitted or required by law and only as part of their official UTPB duties.
- Whenever feasible, Users shall store Confidential Information or other information essential to the mission of UTPB on a centrally managed server, rather than a local hard drive or portable device.
- In cases when a User must create or store Confidential or essential UTPB Data on a local hard drive or a portable device such as a laptop computer, tablet computer, or smart phone, the User must ensure the data is encrypted in accordance with UTPB's and any other applicable requirements.
- The following UTPB 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; and other UTPB Data about an individual likely to expose the individual to identity theft. Email sent to and received from UTPB and other UT System institutions using System and/or System provided email accounts is automatically encrypted. The Information Technology Services department will provide tools and processes for Users to send encrypted data over unsecured networks to and from other locations.

- Users who store UTPB Data using commercial cloud services must use services provided or sanctioned by UTPB, rather than personally obtained cloud services.
- Users must not use security programs or utilities except as such programs are required to perform their official duties on behalf of UTPB.
- All computers connecting to UTPB's network must run security software prescribed by the Information Security Officer as necessary to properly secure UTPB Resources.
- Devices determined by UTPB to lack required security software or to otherwise pose a threat to UTPB Information Resources may be immediately disconnected from the network without notice.

Email

- Emails sent or received by Users in the course of conducting UTPB business are UTPB Data that are subject to state records retention and security requirements.
- Users are to use UTPB provided email accounts, rather than personal email accounts, for conducting UTPB business.
- The following email activities are prohibited when using a UTPB provided email account:
    - 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.
    - 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 UTPB.
    - Sending or forwarding any email that is suspected by the User to contain computer viruses.
    - Any Incidental Use prohibited by this policy.
    - Any use prohibited by applicable UTPB policy.

Incidental Use of Information Resources

- Incidental Use of UTPB Information Resources must not interfere with User's performance of official UTPB business, result in direct costs to UTPB, expose UTPB to unnecessary risks, or violate applicable laws or other UTPB policy.
- Users must understand that they have no expectation of privacy in any personal information stored by a User on a UTPB Information Resource, including UTPB email accounts.
- A User's incidental personal use of Information Resources does not extend to the User's family members or others regardless of where the Information Resource is physically located.
- Incidental Use to conduct or promote the User's outside employment, including self-employment, is prohibited.
- Incidental Use for purposes of political lobbying or campaigning is prohibited.
- 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).
- Files not related to UTPB business may not be stored on network file servers.

Additional Requirements for Portable and Remote Computing

- All electronic devices including personal computers, smart phones or other devices used to access, create or store UTPB Information Resources, including email, must be password protected in accordance with UTPB requirements, and passwords must be changed whenever there is suspicion that the password has been compromised.
- UTPB Data created or stored on a User's personal computers, smart phones or other devices, or in databases that are not part of UTPB's Information Resources are subject to Public Information Requests, subpoenas, court orders, litigation holds, discovery requests and other requirements applicable to UTPB Information Resources.
- UTPB issued mobile computing devices must be encrypted.
- Any personally owned computing devices on which Confidential UTPB Data is stored or created must be encrypted.
- UTPB Data created and/or stored on personal computers, other devices and/or non-UTPB databases should be transferred to UTPB Information Resources as soon as feasible.
- Unattended portable computers, smart phones and other computing devices must be physically secured.
- All remote access to networks owned or managed by UTPB must be accomplished using a remote access method approved by UTPB.

Password Management

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