Acceptable Use Policy

Definitions:

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

General

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

Confidentiality & Security of Data

- Users shall access System Data only to conduct System 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 System data in accordance with System'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 System duties.
- Whenever feasible, Users shall store Confidential Information or other information essential to the mission of the System 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 System 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 System's and any other applicable requirements.
- The following System 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 System Data about an individual likely to expose the individual to identity theft. Email sent to and received from System and UT System institutions using System and/or System provided email accounts is automatically encrypted. The Office of Technology and Information Services will provide tools and processes for Users to send encrypted data over unsecured networks to and from other locations.
- Users who store System Data using commercial cloud services must use services provided or sanctioned by System, 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 System
- All computers connecting to a System's network must run security software prescribed by the Information Security Officer as necessary to properly secure System Resources.
- Devices determined by System to lack required security software or to otherwise pose a threat to System Information Resources may be immediately disconnected by the System from a System network without notice.

Email

- Emails sent or received by Users in the course of conducting System business are System Data that are subject to state records retention and security requirements.
- Users are to use System provided email accounts, rather than personal email accounts, for conducting System business.
- The following email activities are prohibited when using a System 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 System.
- 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 System policy.

Incidental Use of Information Resources

- Incidental Use of System Information Resources must not interfere with User’s performance of official System business, result in direct costs to the System, expose the System to unnecessary risks, or violate applicable laws or other System policy.
- Users must understand that they have no expectation of privacy in any personal information stored by a User on a System Information Resource, including System 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 System 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 System Information Resources, including email, must be password protected in accordance with System requirements, and passwords must be changed whenever there is suspicion that the password has been compromised.
- System Data created or stored on a User’s personal computers, smart phones or other devices, or in data bases that are not part of System’s Information Resources are subject to Public Information Requests, subpoenas, court orders, litigation holds, discovery requests and other requirements applicable to System Information Resources
- System issued mobile computing devices must be encrypted.
- Any personally owned computing devices on which Confidential System Data is stored or created must be encrypted.
- System Data created and/or stored on personal computers, other devices and/or non-System data bases should be transferred to System 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 System must be accomplished using a remote access method approved by the System.

Password Management

- System 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.