UNIVERISTY ACCEPTABLE USE AND SECURITY POLICY

Each individual granted access to data and hard copy information holds a position of trust and must preserve the security and confidentiality of the Information he/she uses. Users of Texas Health and Science University's (THSU) data and information are required to abide by all applicable Federal and State guidelines and THSU's internal policies regarding confidentiality of data,. Including, but not limited to the Family Education Rights and Privacy Act (FERPA); Graham Leach Bliley (GLB); The Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Occupational Safety and Health Administration (OSHA).

Definitions	University: Texas Health and Science University (THSU). University Information Resources: All computer and telecommunications equipment, software, data, and media, owned or controlled by University or maintained on its behalf. University Data: All data or information held on behalf of University, created as result and/or in support of University business, or residing on University Information Resources, including paper records. Confidential Data or Confidential Information: All University Data that is required to be maintained as private or confidential by applicable law. User: Any individual granted access to University Information Resources.
General	University Information Resources are provided for the purpose of conducting the business of University. However, Users are permitted to use University Information Resources for use that is incidental to the User's official duties to University (Incidental Use) as permitted by this policy. Users who are University employees, including student employees, or who are otherwise serving as an agent or are working on behalf of the University have no expectation of privacy regarding any University Data they create, send, receive, or store on University owned computers, servers, or other information resources owned by, or held on behalf, of University. University may access and monitor its Information Resources for any purpose consistent with University's duties and/or mission without notice. Users have no expectation of privacy regarding any University Data residing on personally owned devices, regardless of why the Data was placed on the personal device. All Users must comply with applicable University and System Information Resources Use and Security policies at all times. Users shall never use University Information Resources to deprive access to individuals otherwise entitled to access University Information; to circumvent University computer security measures; or, in any way that is contrary to the University's mission(s) or applicable law. Users must not interfere with the activities of others or use a disproportionate share of information resources. Examples of inappropriate use of resources are shown below. These actions frequently result in complaints and subsequent disciplinary action.

	Sending an unsolicited message(s) to a large number of recipients (known as "spamming the network"). Use of University Information Resources to intentionally access, create, store, or transmit sexually explicit materials is prohibited. Users should report misuse of University Information Resources or violations of this policy. How an incident is reported depends upon the nature of the incident: If Users believe that their personal safety is threatened, they may call the Campus Security Officer. The Campus Security Officer for Austin is Antonio Holloway. He can be reached at 512-444-8082, or faid@thsu.edu. The Campus Security Officer for San Antonio is Kai Chan. He can be reached at 210-509-8080, or asia@thsu.edu. For other incidents, Users should call the Campus Chief Information Security Officer.. For reporting problems with "spam" or unsolicited mail, Users may notify the Internet service provider (ISP) from which the mail was sent.
Confidentiality & Security of Data	Users shall access University Data only to conduct University 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 University data in accordance with University's Records Retention Policy and Records Management Guidelines. Users must not use or disclose Confidential University Data, or data that is otherwise confidential or restricted, without appropriate authorization. Examples of groups that can provide appropriate authorization include, but are not limited to Office of Admissions, Financial Aid, Registrar, Human Resource Services, Offices of the VPs, and Information Security Officer. Users must ensure any individual with whom Confidential University Data is shared is authorized to receive the information. Users may not share University Confidential Data with friends or family members. Users may not share university business data that may be classified as Confidential Data, such as the status of negotiations, terms of contracts, and new research or products or relationships under development. Users will not include or cause to be included in any record or report, a false, inaccurate or misleading entry known to the User. Users will comply with the university's agreements to protect vendor information such as software code, proprietary methodologies, and contract pricing. If Users receive a non-routine request for University Confidential Data from a third party outside of the university, check with an appropriate group within the university to make sure the release of the data is permitted.

	Users must report violations of university policies regarding use and/or disclosure of confidential or restricted information to the Information Security Officer. Confidential or essential University Data stored on a local hard drive or a portable device such as a laptop computer, tablet computer, or, smart phone, must be encrypted. All Confidential University Data must be encrypted during transmission over a network. Users who store University Data using commercial cloud services must only use service approved by the University. Users must not try to circumvent login procedures on any University Information Resource or otherwise attempt to gain access where they are not allowed. Users may not deliberately scan or probe any University Information Resource without prior authorization. Devices determined by University to lack required security software or to otherwise pose a threat to University Information Resources may be immediately disconnected by the Chief Security Information Officer.
Email	Emails sent or received by Users in the course of conducting University business are University Data that are subject to records retention and security requirements. Users are to use University provided email accounts, rather than personal email accounts, for conducting University business. The following email activities are prohibited when using a University 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 University. Sending or forwarding any email that is suspected by the User to contain computer viruses. Any Incidental Use prohibited by this policy.
Incidental Use of Information Resources	Incidental Use of University Information Resources must not interfere with User's performance of official University business, result in direct costs to the University, expose the University to unnecessary risks, or violate applicable laws or other University or 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 University 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.

	Users may not be paid, or otherwise profit, from the use of any university-provided information resource or from any output produced using it. Users may not promote any commercial activity using university information resources. Examples include, attempting to sell football tickets or used text books via the UT course management service or advertising a "Make Money Fast" scheme via a newsgroup. Such promotions are considered unsolicited commercial spam and may be illegal as well. 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.
Additional Requirements for Portable and Remote Computing	All electronic devices including personal computers, smart phones or other devices used to access, create or store University Information Resources, including email, must be password protected in accordance with university requirements, and passwords must be changed every 90 days or whenever there is suspicion that the password has been compromised. University Data should never be created or stored on a User's personal computers, smart phones or other devices. Any data, or in data bases that are not part of University's Information Resources are subject to subpoenas, court orders, litigation holds, and discovery requests. University issued mobile computing devices must be encrypted. Any personally owned computing devices on which Confidential University Data is stored or created must be encrypted. University Data created and/or stored on personal computers, other devices and/or non-University databases should be transferred to University Information Resources as soon as feasible. Unattended portable computers, smart phones and other computing devices must be physically secured.
Password Management	University issued or required passwords, including digital certificate passwords, Personal Identification Numbers (PIN), Digital Certificates, Security Tokens (i.e. Smartcard) from third party servicers, must be maintained securely and shall not be shared or disclosed to anyone. Users must not give others access to University Information Resources unless they are authorized and authenticated for such access. Users may not extend access to university information resources to others without permission. Each User will be held responsible for all activities conducted using the User's password or other credentials.