5.8.10 Information Resources Acceptable Use and Security Policy

Chapter 5 - Information Technology	Original Effective Date: June 2003
Section: 5.8 Information Security	Date Last Reviewed: February 2023
Responsible Entity: Chief Information Security Officer	Date Last Revised: August 2018

I. Purpose

To define the acceptable use of information technology resources.

II. Scope

This policy applies to all current and former faculty, staff, students, residents, healthcare providers, researchers, contractors, or any other third party entities who have direct or indirect access to Information Resources created, held or maintained by UT Health San Antonio or any controlled affiliate, including, but not limited to its clinics, hospitals, and research operations.

III. Policy

A. General

1. University Information Resources are provided for the purpose of conducting the business of UT Health San Antonio (UTHSA) and/or System. However, Users are permitted to use UTHSA Information Resources for use that is incidental to the User's official duties to UTHSA or System (Incidental Use) as permitted by this policy.
2. Users who are UTHSA employees, including student employees, or who are otherwise serving as an agent or are working behalf of the UTHSA have no expectation of privacy regarding any UTHSA Data they create, send, receive, or store on UTHSA owned computers, servers, or other information resources owned by, or held on behalf, of the University. University may access and monitor its Information Resources for any purpose consistent with UTHSA's duties and/or mission without notice.
3. Users have no expectation of privacy regarding any UTHSA Data residing on personally owned devices, regardless of why the data was placed on the personal device.

4. All Users must comply with applicable UTHSA and System Information Resources Use and Security policies at all times.
5. Users shall never use UTHSA Information Resources to deprive access to individuals otherwise entitled to access UTHSA Information, to circumvent UTHSA computer security measures; or, in any way that is contrary to UTHSA's mission(s) or applicable law.
6. Use of UTHSA 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 the UTHSA and is approved in writing by the President or a specific designee. Viewing, access to, or 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 UTHSA and do not express the opinion or position of the UTHSA. An example of an adequate disclaimer is:
    (1) "The opinions expressed are my own, and not necessarily those of my employer, The University of Texas Health Science Center at San Antonio."
8. Users should report misuse of UTHSA Information Resources or violations of this policy to their supervisors.

B. Confidentiality and Security of Data

1. Users shall access UTHSA Data only to conduct UTHSA 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. Users shall maintain all records containing UTHSA Data in accordance with UTHSA's Records Retention Policy and Records Management Guidelines.
3. Users shall not disclose Confidential Data except as permitted or required by law and only as part of their official UTHSA duties.
4. Users must store Confidential Information or other information essential to the mission of UTHSA on a centrally managed server, rather than a local hard drive or portable device. If this is not feasible, the Information Security Officer will need to approve the alternative storage location.
5. In cases when a User must create or store Confidential or essential UTHSA 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 UTHSA, System's and any other applicable requirements.
6. The following UTHSA Data must be encrypted during transmission over an unsecured network:
    a. Social Security Numbers;

b. Personally identifiable medical and medical payment information;

c. Driver's license numbers and other government issued identification numbers;

d. Education records subject to the Family Educational Rights & Privacy Act (FERPA);

e. Credit card or debit card numbers, plus any required code or PIN that would permit access to an individual's financial accounts;

f. Bank routing numbers;

g. And other UTHSA Data about an individual likely to expose the individual to identity theft.

7. Email sent to and received from System and UT System institutions using UTHSA and/or System provided email accounts is automatically encrypted. Information Management and Services will provide tools and processes for Users to send encrypted data over unsecured networks to and from other locations.

8. Users who store UTHSA Data using commercial cloud services must use services provided or sanctioned by UTHSA, 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 the UTHSA.

10. All computers connecting to a UTHSA's network must run security software prescribed by the Information Security Officer as necessary to properly secure UTHSA Resources.

11. Devices determined by UTHSA to lack required security software or to otherwise pose a threat to UTHSA Information Resources may be immediately disconnected by UTHSA from a UTHSA network without notice.

C. Email

1. Emails sent or received by Users in the course of conducting UTHSA business are UTHSA Data that are subject to state records retention and security requirements.

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

3. The following email activities are prohibited when using a UTHSA 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:

i. As part of an authorized investigation;

ii. As part of an approved monitoring process; or

iii. For other purposes specifically associated with the User's official duties on behalf of UTHSA.

c. Sending or forwarding any email that is suspected by the User to contain computer viruses.

d. Any Incidental Use prohibited by this policy.

e. Any use prohibited by applicable UTHSA or System policy.

D. Incidental Use of Information Resources

1. Incidental Use of UTHSA Information Resources must not interfere with User's performance of official UTHSA business, result in direct costs to UTHSA, expose UTHSA to unnecessary risks, or violate applicable laws or other UTHSA or System policy.
2. Users must understand that they have no expectation of privacy in any personal information stored by a User on a System Information Resource, including UTHSA email accounts.
3. 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 Resources 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 System business may not be stored on network file servers.

E. Additional Requirements for Portable and Remote Computing

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

4. Any personally owned computing devices on which Confidential UTHSA Data is stored or created must be encrypted.
5. UTHSA Data created and/or stored on personal computers, other devices and/or non-UTHSA databases should be transferred to UTHSA Information Resources as soon as feasible.
6. Unattended portable computers, smart phones and other computing devices must be physically secured.
7. All remote access to networks owned or managed by UTHSA or System must be accomplished using a remote access method approved by UTHSA or System, as applicable.

F. Password Management

1. UTHSA 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 credentials.

IV. Definitions

When used in this document, the following words have the meaning set forth below unless a different meaning is required by context.

UTHSA - The University of Texas Health Science Center at San Antonio (DBA UT Health San Antonio)

System - The University of Texas System

UTHSA Information Resources - All computer and telecommunications equipment, software, data, media and intellectual property owned or controlled by UTHSA or maintained on its behalf.

UTHSA Data - All data information or intellectual property held on behalf of UTHSA, created as a result and/or in support of UTHSA business, or residing on UTHSA Information resources, including paper records.

Confidential Data or Confidential Information - All UTHSA data and intellectual property that is required to be maintained as private or confidential by applicable law.

User - Any individual granted access to UTHSA Information Resources.

V. Related References

There are no related documents associated with this Policy.

VI. Review and Approval History

A. The approving authority of this policy is the University Executive Committee.

B. The review frequency cycle is set for three years following the last review date, a time period that is not mandated by regulatory, accreditation, or other authority.

Effective Date	Action Taken	Approved By	Date Approved
06/2003	Policy Origination		
08/2018	Policy Revision		
02/2023	Policy Review/Discretionary Edit		