Chapter 5	Information Management & Services	Effective:	June 2003
Section 5.8	Information Security	Revised:	October 2016
Policy 5.8.10	**Information Resources Acceptable Use and Security Policy**	Responsibility:	Chief Information Security Officer

INFORMATION RESOURCES ACCEPTABLE USE AND SECURITY POLICY

Scope

All individuals granted access to or use of System Information Resources must be aware of and agree to abide by the following acceptable use requirements.

Definitions

UNIVERSITY: The University of Texas Health Science Center at San Antonio (DBA UT Health San Antonio)

SYSTEM: The University of Texas System

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 a 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 and/or System. However, Users are permitted to use University Information Resources for use that is incidental to the User's official duties to University or System (Incidental Use) as permitted by this policy.

Users have no expectation of privacy regarding any University Data residing 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.

Use of University 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 University 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.

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 University and do not express the opinion or position of University. An example of an adequate disclaimer is:

"The opinions expressed are my own, and not necessarily those of my employer, The University of Texas Health Science Center at San Antonio."

Users should report misuse of University Information Resources or violations of this policy to their supervisors.

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

Users must store Confidential Information or other information essential to the mission of University 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.

In cases when a User must create or store Confidential or essential University 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 University, System's and any other applicable requirements.

The following University 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 University Data about an individual likely to expose the individual to identity theft.

Email sent to and received from System and UT System institutions using University 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.

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

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

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 University from a University network without notice.

Email

Emails sent or received by Users in the course of conducting University business are University Data that are subject to state 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.
- Any use prohibited by applicable University or System 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.

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 University information Resources, including email, must be password protected in accordance with University requirements, and passwords must be changed whenever there is suspicion that the password has been compromised.

University Data created or stored on a User's personal computers, smart phones, or other devices, or in data bases that are not part of University's Information Resources are subject to Public Information Requests, subpoenas, court orders, litigation holds, discover requests and other requirements applicable to University Information Resources.

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 data bases should be transferred to University 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 University or System must be accomplished using a remote access method approved by the University or System, as applicable.

Password Management

University 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.

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