5.8.31 Cloud Computing Policy

Chapter 5 - Information Technology	Original Effective Date: October 2016
Section: 5.8 Information Security	Date Last Reviewed: February 2023
Responsible Entity: Chief Information Security Officer	Date Last Revised:

I. Purpose

To establish policy and standards for storing Institutional data in a third-party cloud computing system.

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

Data that is stored, managed or processed on Cloud Computing and Storage Services (Cloud) is subject to all UT Health San Antonio (UTHSA) Policies, Standards and Procedures and state and federal laws and regulations.

A. All use of Cloud services must be approved by the Chief Information Security Officer.

   1. Users may not enter into Cloud service contracts on behalf of UTHSA, including free or trial term service agreements; and
   2. Data may not be transmitted or stored on personally procured Cloud services.

B. Cloud services processing confidential or regulated data shall be classified as High Risk.

C. It is the responsibility of the Information Resource Owner to ensure the use of Cloud services is in compliance with UTHSA Policies, Standards and Procedures, as well as applicable state and federal laws.

1. Authentication for Cloud services must comply with the UTHSA "Access Management" policy as stated in 5.8.4 of the Handbook of Operating Policies (HOP), including use of two-factor authentication for confidential and mission critical data.
2. Use of Cloud services is subject to the UTHSA "Security Monitoring" policy 5.8.13 of the HOP, Standards and Procedures.
    a. Information Management and Services may restrict or filter access to unapproved Cloud services.

D. The Chief Information Security Officer shall execute a Risk Assessment prior to initial purchase or use of the Cloud service and on no less than an annual basis thereafter. The Risk Assessment may include:

1. documentation of common security controls used by the Cloud service vendor and determination if the vendor has sufficient technological, administration and physical safeguards to ensure the confidentiality, security and integrity of the data stored by the Cloud service; and
2. penetration test of the Cloud service perimeter network and application services.
3. The Cloud service vendor may provide to the Chief Information Security Officer any independent third-party vulnerability assessments, audits or penetration tests to satisfy UTHSA Risk Assessment Policy and Standards requirements.

E. Cloud services must make available a technical administration control or process and/or have a contractual provision to allow a UTHSA Information Security Administrator to retrieve data in the event a Cloud User is no longer associated with the University and upon termination of the contract with the Cloud service.

F. Upon termination of a User or the contract, the Cloud service vendor must return or securely destroy all UTHSA data in its possession, as determined by UTHSA.

In the event that returning or securely destroying the data is not feasible, the Cloud service vendor must provide notification of the conditions that make destruction infeasible, in which case the vendor must:

a. continue to protect all data that it retains;
b. agree to limit further uses and disclosures of such data to those purposes that make the destruction infeasible for as long as it maintains the data; and
c. to the extent possible, de-identify the data.

G. Contract agreements with Cloud service vendors must include statements to ensure they comply with HIPAA, FERPA, PCI and any other state or federal laws and regulations that may govern the use and access of data stored on the Cloud service.

IV. Definitions

There are no defined terms used in this Policy.

V. Related References

U.T. System (UTS) Policy
UTS 165 Information Resources Use and Security, Standard 11: Safeguarding Data.

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
10/2016	Policy Origination		
02/2023	Policy Review		