Chapter 5	Information Management & Services	Effective:	October 2016
Section 5.8	Information Security	Revised:	
Policy 5.8.31	**Cloud Computing Policy**	Responsibility:	Chief Information Security Officer

CLOUD COMPUTING POLICY

Policy

Data that is stored, managed or processed on Cloud Computing and Storage Services (Cloud) is subject to all UT Health San Antonio 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.

   i. Users may not enter into Cloud service contracts on behalf of UT Health San Antonio, including free or trial term service agreements; and

   ii. Data may not be transmitted or stored on personally procured Cloud services.

b. All Cloud services 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 UT Health San Antonio Policies, Standards and Procedures.

   i. Authentication for Cloud services must comply with the UT Health San Antonio "Access Management" policy as stated in Section 5.8.4 of the *Handbook of Operating Procedures* (HOP), including use of two-factor authentication for confidential and mission critical data.

   ii. Use of Cloud services is subject to the UT Health San Antonio "Security Monitoring" policy, Section 5.8.13 of the HOP, Standards and Procedures.

      - 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:

i. 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

ii. penetration test of the Cloud service perimeter network and application services.

The Cloud service vendor may provide to the Chief Information Security Officer any independent third-party vulnerability assessments, audits or penetration tests to satisfy UT Health San Antonio 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 UT Health San Antonio 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 UT Health San Antonio data in its possession, as determined by UT Health San Antonio.

i. 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:

i. continue to protect all data that it retains;

ii. 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

iii. 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.

Reference

- U.T. System Policy 165 Standard 11