OIS 49 – Standard for Cloud Computing

I. STANDARD STATEMENT

Prior to acquiring services from Cloud Services Providers, The University of Texas at San Antonio will assess information security risk and present the results to the President-delegated Authorities.

II. RATIONALE

This standard provides university leadership the ability to select a Cloud Services provider with the full knowledge of information security risks and to ensure security controls are in place.

III. SCOPE

This standard applies to UTSA faculty and staff that acquire services from Cloud Services providers on behalf of the university.

IV. CONTACTS

informationsecurity@utsa.edu

V. Responsibilities

A. Data Owner – Identified person who will manage the lifespan of the contract with the Cloud Services provider.
B. Cloud Services Provider – A third party provider such as Software as a Service or Hardware as a Service. These providers host information resources that process or store university data on behalf of the university and in facilities outside of university control.
C. Cloud Services - The practice of using a network of remote services hosted outside UTSA to store, manage, or process data, rather than local UTSA information resources.
D. User - Any individual granted access to University Information Resources and/or University Data.

E. President-delegated Authority - Only an individual with a written delegation of authority from the President of UTSA may execute and deliver contracts on behalf of the University.
F. University Data - All data or information held on behalf of the university or created as a result and/or in support of university business, including paper records. The university does not assert an ownership interest in the content of exclusively personal information or documents stored on University Information Resources as part of a User's Incidental Use.

VI. Standards

A. University data stored at Cloud Services must be stored on only UTSA approved third-party services (UTS165: Standard 11.2: Safeguarding Data - Non-University Third-Party Storage Services).
B. Users who are not President-delegated Authorities must not enter into Cloud Services contracts on behalf of the university. Many Cloud Services typically include "click-to-accept" agreements and introduce risks regarding university information. Entering into such agreements--even if the service is free—on behalf of the university is prohibited.
C. Use of Cloud Services must comply with all other university policies standards, and procedures. It is the responsibility of the user to ensure that the use is consistent with UTSA policies.
D. Cloud Services procured or used by the university must have a mechanism to allow a university administrator to retrieve the university data in the event a cloud user is no longer associated with the university. For example, a UTSA administrator with an enterprise cloud administrator account with permissions to reset passwords or reassign accounts must be able to reset passwords or reassign user accounts.
E. Cloud Services procured or used by the university must comply with the published university standards.
F. Data Owners must contact the UTSA Purchasing and Contracts departments to initiate the information security review of the intended Cloud Services provider and/or the use of Cloud Services.
G. Cloud Services vendors with access to university data must enter into the appropriate legal agreements with the university to support HIPAA, FERPA, TAC 202, and any other regulations with which the university is required to comply.

Title: OIS 49 – Standard for Cloud Computing
Effective Date: 12/1/2017
Last Reviewed: 08/10/2020