HSC OP: 56.05, Cloud Computing

PURPOSE: The purpose of this Operating Policy (OP) is to define the specific information security requirements for the establishment of and use of cloud services to store or manage TTUHSC information assets without jeopardizing TTUHSC data and computing resources. This policy applies to all faculty, staff, and students for all external cloud services (e.g., cloud-based email, document storage, Software-as-a-Service (SaaS), Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), etc.). Personal email accounts are excluded.

REVIEW: This OP will be reviewed annually in December by the TTUHSC Chief Information Officer (CIO) and the Information Security Officer (ISO).

TABLE OF CONTENTS:
1. Cloud Approval and Governance ....................................................................................................................2
   a. Approval Required ..........................................................................................................................................2
   b. Vendor Validation ...........................................................................................................................................2
   c. Control Compliance ........................................................................................................................................2
2. Establishing Cloud Services ...........................................................................................................................2
   a. Terms of Service Approval .............................................................................................................................2
   b. Only Preapproved Cloud Services .................................................................................................................2
3. Access Controls ...............................................................................................................................................2
   a. Access Credentials .........................................................................................................................................2
   b. Password Sharing ...........................................................................................................................................2
   c. Management Reporting ..................................................................................................................................2
4. Privacy Controls ...............................................................................................................................................3
5. Sensitive Data Storage .....................................................................................................................................3
   a. Data Storage Approval ...................................................................................................................................3
   b. Personal Data Storage ...................................................................................................................................3
6. Violations ...........................................................................................................................................................3
   a. Disciplinary Repercussions .............................................................................................................................3
Related Statutes, Policies, and Requirements ......................................................................................................4
IT Division Document Details ..................................................................................................................................5
POLICY:

1. Cloud Approval and Governance
   a. Approval Required

   The TTUHSC Information Technology Division has established Box as the institutional cloud storage service. Use of any other third-party cloud computing services for TTUHSC business purposes must be authorized by the CIO and ISO, or their designee. Employees must not open cloud services accounts or enter into cloud service contracts for the storage, manipulation, or exchange of TTUHSC-related communications or TTUHSC-owned data without approval.

   b. Vendor Validation

   All cloud vendors must be approved by the IT Division. The ISO must verify that security, privacy, and all other IT Division management requirements will be adequately addressed by the cloud computing vendor.

   c. Control Compliance

   Additional regulatory control requirements adopted as part of cloud arrangements must be formally adopted into the TTUHSC internal control framework.

2. Establishing Cloud Services
   a. Terms of Service Approval

   For any cloud services that require users to agree to terms of service, such agreements must be reviewed and approved by the TTUHSC Contracting Office.

   b. Only Preapproved Cloud Services

   Employees must only establish cloud service accounts with approved cloud service vendors that have been approved by the ISO. At this time, Box is the only allowed cloud storage vendor for TTUHSC. Exceptions may be granted for research and medical-related purposes. These exceptions must also be approved by the CIO or their designee.

3. Access Controls
   a. Access Credentials

   Employees and contractors establishing login credentials with cloud service vendors must comply with existing TTUHSC security requirements for secure passwords.

   b. Password Sharing

   Employees and contractors establishing login credentials with cloud service vendors must not share passwords.

   c. Management Reporting

   Employees and contractors that establish login credentials with approved third-party alternate cloud service vendors must notify their manager and the IT Division of the details of the account and the
4. Privacy Controls
   a. Foreign Data Transfer
      Customer and patient personally identifiable information (PII) or electronic patient health
      information (ePHI) must not be stored in cloud environments that are located in foreign countries.

5. Sensitive Data Storage
   a. Data Storage Approval for Alternate Third-party Cloud Environments
      The CIO, in conjunction with the ISO, must approve the types of data that may be stored in alternate
      third-party cloud environments.
   b. Personal Data Storage
      Personal cloud services accounts may not be used for the storage, manipulation, or exchange of
      TTUHSC-related communications or TTUHSC-owned data.

6. Violations
   Any violation of this policy may result in disciplinary action, up to and including termination of employment.
   TTUHSC reserves the right to notify the appropriate law enforcement authorities of any unlawful activity
   and to cooperate in any investigation of such activity.
   a. Disciplinary Repercussions
      Misuse of TTUHSC IR is a violation of the policies contained herein and can result in disciplinary
      action in accordance with, but not limited to, TTUHSC OPs 70.31 “Employee Conduct, Coaching,
      Corrective Action, and Separation from Employment” and 77.05 “Suspension and Retention,” as
      well as the Student Handbook.
Related Statutes, Policies, and Requirements

Digital Millennium Copyright Act
Digital Millennium Copyright Act of 1998

Family Educational Rights and Privacy Act (FERPA)
General FERPA details

FERPA, related to TTUHSC

Health Insurance Portability and Accountability Act
HIPAA, Title 45, Subchapter C, Part 164

Payment Card Industry (PCI) Data Security Standard (DSS)
PCI-DSS: 12.3 Acceptable Usage

Texas Administrative Code
TAC 202, Subchapter C, 70-76

Texas Public Information Act
Texas Public Information Act

Texas Security Control Standards Catalog
Texas DIR Security Control Standards Catalog

TTUHSC IT Areas of Responsibility
Areas of Responsibility
IT Division Document Details

Approval and Ownership

<table>
<thead>
<tr>
<th>Approved By</th>
<th>Vince Fell</th>
</tr>
</thead>
<tbody>
<tr>
<td>Title</td>
<td>Vice President for Information Technology and Interim Chief Information Officer</td>
</tr>
<tr>
<td>Approval Date</td>
<td>December 20, 2017</td>
</tr>
<tr>
<td>Owner(s)</td>
<td>IT Executive Management Team</td>
</tr>
</tbody>
</table>

Revision History

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
<th>Date Reviewed</th>
<th>Date Submitted for Publishing</th>
<th>Reviewer(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>Initial version.</td>
<td>11/17/2017</td>
<td>12/20/2017</td>
<td>Andrew Howard</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Shayla Corprew</td>
</tr>
</tbody>
</table>