Use of Third Party and Hosted Information Services **POLICY**

Implementation Date: 6/19/2017

Definition

Hosted "Cloud" services are applications, infrastructure and information resources hosted off-campus which are accessed via the internet. Cloud computing resources range from off-campus file storage services such as Box.com or Dropbox.com, to hosted email such as Gmail.com, or Exchange.csusm.edu, to special purpose services that provide specific functionality. Examples include but are not limited to complex multi-purpose cloud applications such Google Apps for Education and Microsoft Office 365, along with more narrowly focused application such as ICIMS or Maxient.

These resources are vital for the fulfillment of the academic, research and business needs of the campus. This policy ensures that campus information assets hosted in the cloud, along with applications and services offered by third parties are managed and protected in a manner consistent with on-campus systems. This policy addresses the review and approval process for purchase, contract or "free" use of hosted or third party information technology resources for purposes related to the campus mission.

Authority

CSUSM President

Scope

This policy is intended to apply to all hosted or third party applications used to provide computing, application or network services, platforms, and infrastructure for campus operations. The policy is intended to apply to a wide range of services which involve access, exchange, storage, processing or analysis of campus data regardless of whether it is a free or contracted service or resource.

Karen S. Haynes, President

6/19/2017
Date

Implementation Date: 6/19/2017

I. BACKGROUND

A. Many of the technology functions and services formerly available only on the campus network are now widely available on the Internet.

B. Many cloud services are offered (perhaps in a minimal version) for free. Others may require a monthly charge or small fee. Most cloud services require individual users to accept click-through agreements. These agreements often fail to address the required protections for campus data.

C. Use of these unapproved resources for campus business purposes may expose the campus to risk and liability. It is a violation of CSU policy, and in some cases state and federal law, to store data or provide access to unauthorized third parties.

D. Risks with using unauthorized cloud and/or third-party services include, but are not limited to:

- Unauthorized access to sensitive or confidential data
- Use of campus data by third parties without the consent of the university
- Loss of campus data
- Failure to comply with storage or access requirements for campus data

II. Policy

A. Only authorized third-party or hosted services may be used to access, exchange, store, process or analyze campus data, or to provide the campus with critical operational technologies.

B. Only Procurement Services is authorized to contract with third-party or hosted service providers for paid or free services.

C. The campus Information Security Officer must approve the use of third-party or hosted services which access, store or process protected campus data.

III. Procedure

A. Individuals contemplating use of a hosted or third-party technology application must first contact IITS.

B. IITS assists the organization to identify a solution which meets or exceeds the following criteria:

a) The solution must be operationally and/or technically feasible
b) Must be significantly unique; i.e. different from any existing application or function
c) Required due to business process needs

C. IITS works with requesting organization to prepare application/service information sheet providing basic data such as:

a) Nature of data to be accessed, stored or processed
b) Description of use
c) Authentication method
d) Description of application or service
e) Compliance documentation with respect to the CSU Accessible Technology Initiative (ATI)

D. Within three (3) working days, the Information Security Office performs the initial risk assessment to determine the risk level of the information system. If the initial risk assessment determines that there is significant risk, a formal risk assessment will be completed within thirty (30) days and a copy provided to the requestor(s).
E. If the campus decides to purchase the system:
   a) The Information Security Office may provide recommendations as to contract elements required to meet security considerations.
   b) Procurement works with the vendor to assure appropriate contract clauses are included, and that all appropriate documentation has been completed.
F. Upon receipt of the new system:
   a) IITS works with department to ensure configuration, implementation and support requirements are met.

IV. Controls

A. Upon receipt of a request to evaluate procurement of a new information system, the messages are documented in the shared folder titled "Procurement Approval Controls."