CALIFORNIA STATE UNIVERSITY
SAN BERNARDINO

CSUSB Cloud Computing Standard
CSUSB, Information Security Office

Last Revised: **01/30/2013**

Final

REVISION CONTROL

Document Title: CSUSB Cloud Computing Standard

Author: James Macdonell

File Reference:

Date	By	Action	Pages
05/04/12	J Macdonell	Created Standard	All

Review/Approval History

Date	By	Action	Pages
			All

1.0 Cloud Computing Standard

CSUSB
Cloud Computing Standard

Introduction

Cloud computing refers to computing services that include Infrastructure Hosting Services, Application Hosting or Software as a Service (SaaS), and any other computing services which are administered and maintained by a third party contractor and are typically external to the University network.

The CSU and CSUSB have adopted a data classification standard that identifies the sensitive information elements that require the very highest level of information security protection (confidentiality, integrity, availability) in order to meet compliance requirements with applicable federal and state laws. In addition, CSU and CSUSB computer services must also comply with the requirements of accessibility of information as required by the American Disability Act (ADA), and with information security requirements, such as disclosure of non-public information and incident handling, and retention and preservation of University information in case of an eDiscovery or litigation hold.

Purpose

The purpose of this standard is to provide the minimum requirements that should be taken in consideration when evaluating a cloud computing service. However, it is recommended that a full risk assessment should be conducted before a final purchase decision or contract is signed. This standard is applicable in all cases when a cloud computing service or an on-line tool is used to conduct an academic activity or business process.
In cases when university employees make a decision to use cloud computing applications or on-line tools, because the service plays an important roles in the execution of an important academic activity or business process, the individuals should take into consideration privacy and security and ensure the service meets all the applicable information security protections and requirements including CSU and CSUSB accessibility requirements.
Cloud computing services that will be used for instructional purposes should be carefully considered and ensure meet all the security and accessibility requirements described in this standard.

Confidential institutional data or otherwise sensitive institutional business records, such as information protected under the Family Educational Rights and Privacy Act (FERPA), **must not be stored, shared, or otherwise processed** by a cloud computing service unless the service enters into a legally binding agreement with the university to protect and manage the data according to standards and procedures acceptable to CSUSB and in compliance with the CSU Information Security Policy.

Definitions

Cloud computing services include the use of the following services and/or technologies:
• External services e.g., Hotmail, Gmail, Yahoo Mail, iCloud, DropBox, etc.
• Chat, Instant Messaging and Telephony Services such as Yahoo, AIM, MSN, IRC, Twitter, Skype, etc.
• Social Networking Services (such as MySpace, FaceBook, YouTube, Friendster, etc.
• Hosted Application Services such as Google Apps for Education, Amazon Web Services, etc. ◦ Peer to Peer File Sharing such as Kazaa, Gnutella, Bit Torrent, LimeWire, Morpheus, etc.
◦ Virtual Machines such as GoGrid and Amazon Elastic Compute Cloud, which are commercial web services that allow customers to rent any number of virtual computers upon which they can load and run their own software application.

Scope

This standard applies to all academic and administrative departments, including auxiliaries.
Information Technology Standards

The following requirements are intended to assist in the evaluation of cloud computing services and ensure the service will meet CSU and CSUSB requirements.

1. Consult with appropriate data custodian for the appropriateness of the use of any institutional data.

2. Ensure cloud computing applications and services are assessed and meet the CSU and CSUSB accessibility requirements, including accessibility requirements for instructional materials.

3. Since cloud computing services are maintained by several parties, clearly define roles and responsibilities of each party and establish a change control process. Include a campus procedure for granting and removing permissions/access to the service.

4. Ensure the service complies with the university use of intellectual property including copyright, trademarks, and patents.

5. If the service will access/store/transmit confidential information, the contract should include:
- Clear definition of services
- a non-disclosure and confidentiality agreement
- a provision to delineate responsibilities to comply with applicable notification laws in case of a security breach
- an agreement to notify the University Information Security Office (ISO) within 24 hours of discovering the incident.
- Confidentiality and non-disclosure agreements for the employees of the service

- Disaster recovery
- The service should only allow secure protocols for the administration.
- The service should fully collaborate with any University investigation, including the release of appropriate log files.
- Fully collaborate with the retention and preservation of University information in case of an eDiscovery or litigation hold, including the release of appropriate log files.
- Authorization for the University to conduct security vulnerability and accessibility assessments of the service as needed in order to meet CSU audit requirements.
- Notify the University within 24 hours in the event that University information is requested by law enforcement or subpoenaed.
- Request authorization from the University prior to using information collected about visitors, content visited, usage profile, etc., for any purpose.
- Dispose of all University information at the end of the contract.
- Develop an exit strategy. Prepare a method to restore data and services in the event the service or the University abruptly ends the contract, the service has a prolonged outage, the service goes out-of-business.

Authorization and Implementation

In most instances cloud computing services require campus network services to be properly configured for their implementation. As part of the university change control process, campus entities must submit a request using the Authorization for Third Party Cloud Computing Services form to the Information Security Office and include documentation that addresses the applicable information technology standards. The Information Security Office will review the documentation for compliance with CSU and CSUSB applicable policies and standards.

2.0 Cloud Computing Authorization Form

CSUSB
Authorization for Third Party Cloud Computing Services

Documentation addressing the applicable information technology considerations describe on the campus Cloud Computing Standard must be submitted to the Information Security Office as part of thisrequest. The Information Security Office will review the documentation to ensure the service complieswith the applicable requirements before the request for service is enabled. The following information is necessary to enable third party cloud computing services:

Points of Contact

_____	_____	_____
Manager (MPP)	Signature	@csusb.edu Email
_____	_____	_____
Campus IT Staff	Signature	@csusb.edu Email

Service Details

Cloud Computing Service	
Cloud Computing Provider	
Description	

Technical Details

Changes to campus IT infrastructure (typically DNS modification)	

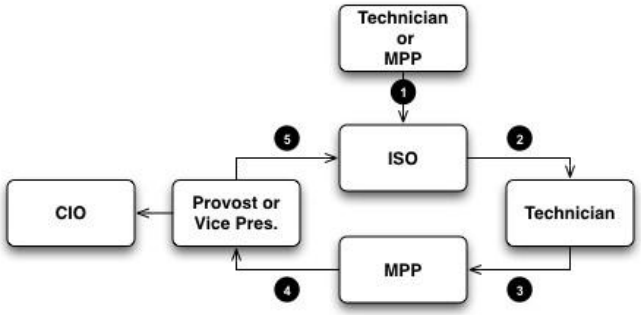
The third party cloud computing provider has been given careful consideration and has addressed the applicable University security controls and requirements. The computing service described in this request is authorized to be provided by the selected third party.

_____	_____	_____
Vice President/Provost	Signature	Preferred Email

Form Instructions

Submission Procedure

Once management as reviewed the considerations for outsourcing and the recommendations for cloud computing and are now seriously considering outsourcing a service, management should proceed as follows:



1. Technician or Manager submits a work order request
2. ISO sends Technician an authorization form. Technician is responsible for "Service Details" and "Technical Details"
3. Technician forwards form to Manager. Manager is responsible for "Points of Contact" and for considering stated recommendations.
4. Manager forwards form to their Vice President or Provost. VP/Provost is responsible for ensuring the service meets university requirements
5. VP/Provost consults with CIO. On approval, VP/Provost forwards completed form to security@infosec.csusb.edu. Email must originate from VP/Provost.

Points of Contact

A campus manager and IT staff need to be identified as points of contact in case of any security and non-compliance issues.

Service Details

Cloud Computing Services

Generic examples: *Web Hosting, Content Versioning, Storage, Email Hosting, Data Processing*
Specific examples: *Sharepoint, Wordpress*

Cloud Computing Provider

Examples: *route66.net, sharepointsite.com, wordpress.com*

Description

Should define the service and how it will be used for University business.

Technical Details

Describe the changes to the campus IT infrastructure necessary to support the service. Typically these are DNS changes.

Example: *Create a new A record, myservice.csusb.edu IN A 172.19.238.11*