# 8065.S003 Information Security Asset Management – Cloud Storage & Services

| | |
|---|---|
| **Implements:** | CSU Policy #8065.0 |
| **Policy Reference:** | http://www.calstate.edu/icsuam/sections/8000/8065.0.shtml |

## Introduction

The purpose of this standard is to ensure that CSU data is appropriately stored or shared using public cloud computing and/or file sharing services.

Cloud computing services are application and infrastructure resources that users access via the Internet. These services enable customers to leverage powerful computing resources that would otherwise be beyond their means to purchase and support. Cloud services provide services, platforms, and infrastructure to support a wide range of business activities.

Employees must not store or transmit protected University data using services hosted by third parties which do not have a contract in place with the campus or its Auxilliaries, such as personal cloud accounts.

There are a number of information security and data privacy concerns about use of cloud computing services by University Personnel, departments, auxiliaries and centers. They include but are not limited to:

- University no longer protects or controls its data, leading to a loss of security, lessened security, or inability to comply with various regulations and data protection laws
- Loss of privacy of data, potentially due to aggregation with data from other cloud consumers
- University dependency on a third party for critical infrastructure and data handling processes
- Potential security and technological defects in the infrastructure provided by a cloud vendor
- University has limited service level agreements for a vendor's services and the third parties that a cloud vendor might contract with
- University is reliant on vendor's services for the security of some academic and administrative computing infrastructure

Note that all requirements from all other relevant CSU policies and standards remain in full effect when cloud services are used.

## 1.0 Definitions

Cloud computing and file sharing, for this purpose, is defined as the utilization of information technology services of any type that is not provided by servers which are owned/leased by the CSU or auxiliaries including, but not limited to, social networking applications, file storage, and content hosting.

The following definitions are taken from NIST Special Publication 800-145, The NIST Definition of Cloud Computing (http://dx.doi.org/10.6028/NIST.SP.800-145).

### 1.1 Software as a Service (SaaS)

The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not

manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

1.2 Platform as a Service (PaaS)

The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.

1.3 Infrastructure as a Service (IaaS)

The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls).

## 2.0 Scope

This standard applies to all uses of Cloud Computing Services by the CSU or auxiliaries.

## 3.0 Asset Management

3.1 Access to Data Stored in the Cloud

Campus information assets stored in the cloud shall be protected with no less control than that used for on-premise systems, as per ICSUAM 8065 Asset Management and associated standards.

3.2 Protected Level One Data Stored in the Cloud

Campuses shall not use cloud services to store protected level one data (i.e. storage hosting solutions such as box.com, dropbox.com, google docs, etc) unless such access can be limited by technical or procedural controls in order to reduce inadvertent exposure. Examples of adequate controls include but are not limited to:

- Configuration options which limit user ability to share documents or folders outside the organization
- Training and awareness for users who store protected level one data
- Periodic reports showing user permissions/access, including:
  - Reports of all access
  - Reports of all access granted to off campus entities
- Periodic assessment of protected level one data stored off campus
- Procedures for the management of encryption keys must protect the keys from unauthorized disclosure.

3.3 Synchronization of Stored Content

Level 1 data stored in a cloud provider may only be automatically synchronized with compliant assets, computers, and devices that are university owned and managed.

## 4.0 Access Control

4.1 Authentication to Cloud Services

Authentication to campus information assets hosted in the cloud shall be subject to no less control than those hosted on campus and must comply with ICSUAM 8060 Access Control and associated standards.

Central Authentication

Web-based SAAS cloud services must use a campus central authentication method in order to ensure that campuses may appropriately provision and deprovision identies and authorization for campus personnel. Examples of this include but are not limited to Shibboleth, SAML, ADFS, and CAS.

Campus authentication services must be configured in such a manner that the cloud provider does not have access to passwords in either text or encrypted format. Examples of protocols that expose user passwords to the service providers include but are not limited to: LDAP and Radius.

When Central Authentication is Unavailable

The campus must establish a procedure for approving web-based SAAS cloud services that do not use central authentication. This procedure must include a documented risk assessment and periodic review of the service. Where campus authentication is not used, the campus must have a way to recover any account when the community member separates, such as using a campus email address as the contact for password resets, maintaining an appropriately protected list of passwords, or having the campus administer the accounts. Additionally, the cloud host may not store passwords in text, or clear text.

4.2 Multi-Factor Authentication

To mitigate the risk of a data breach occurring as a result of compromised credentials (such as through a successful phishing attack), multi-factor authentication is required for access to level one data belonging to someone else from off campus.

## 5.0 Acquisition

5.1 Campuses must establish a process and assign responsibility for ensuring that contracts and renewals for cloud services are reviewed in order to identify appropriate supplemental contract lanaguage.

5.2 A risk assessment may be necessary where 3rd party contract terms substantially deviate from CSU supplemental or general IT terms in such manner as to pose a risk to the confidentiality, integrity, or availability of CSU protected data.

5.3 To assist campuses in responsibly assessing the risk of contemplated cloud purchases, cloud vendors who will be storing or accessing Protected Level 1, 2, or 3 data, or using central authentication must provide the campus with a security plan and/or policy and at least one of the following before the acquisition of any cloud services:

1. A current SSAE-16 SOC 2 Type II (or equivalent third party audited security standard)
   This is a questionnaire that demonstrates the SOC compliance status in the following areas: Security, Availability, Processing Integrity, Confidentiality and Privacy. Each provider must demonstrate adherence to these principles to produce a qualified opinion.

2. A current Cloud Security Alliance Consensus Assessment Initiative Questionnaire (CSA CAIQ)
   This is a questionnaire of about 300 questions used to assist both cloud providers, by providing principles of cloud security standards, and clients looking for appropriate cloud providers to suit their business needs and meet their security standards.

3. The SurveyAnalytics's Standardized Information Gathering Questionnaire
   This questionnaire is used by outsourcers to obtain required documentation on a service provider and establish a profile on operations and controls for each control area.

4. The Higher Education Cloud Vendor Assessment Tool
   This questionnaire is designed specifically to help higher education institutions evaluate the security of cloud vendors.

   The vendor provided information must be referenced in the contract. Campuses can tailor the CSA CAIQ or questionnaire, and the risk assigned to each portion of the CSA CAIQ or questionnaire, as appropriate for each purchase. Examples are provided in Appendix A.

5.4 The requestor must provide a complete description of how they will deploy the product, including the type of data that will be involved and the type of authentication that will be used. A sample format is included in Appendix B.

5.5 Acquisition of cloud services which store, or access, or provided access to protected data must comply with ICSUAM 8040 Managing Third Parties. Informing users: Campus must publish a guideline indicating what types of data may be stored on each cloud storage solution and how each cloud storage solution may be used, and must inform all users of cloud storage of this guideline.

## 6.0 Appendix A

CAIQ Protected Level 1 Cloud Assessment
CAIQ Protected Level 2 Cloud Assessment
CAIQ Protected Level 3 Cloud Assessment

## 7.0 Appendix B

Security Data Requirements Checklist

## REVISION CONTROL

### Revision History

| Version | Revision Date | Revised By | Summary of Revisions | Section(s) Revised |
|---|---|---|---|---|
| 0.1 | 8/3/2015 | CSU Chico | Initial version provided by CSU Chico. | All Sections. |
| 1.0 | 12/13/2016 | Andru Luvisi | Revised all sections. | All Sections |
| 1.1 | 2/17/2017 | Andru Luvisi | Added details on each type of questionaire | Section 5.3 |
| 1.2 | 9/5/2017 | Andru Luvisi | Minor Edits | Sections 3.0-5.0 |
| 1.3 | 5/7/2020 | Leslie DeCato | Revised URL for HECVAT | Section 5.0 |

### Review / Approval History

| Review Date | Reviewed By | Action (Reviewed, Recommended or Approved) |
|---|---|---|
| 1/06/2017 | W. Perry | Reviewed and Approved |
| 2/22/2017 | W. Perry | Reviewed: Submitted to ITAC/ISAC Review Timeframe: 02/24/17 until 03/24/17. |
| 9/5/2017 | E. Hudson | Reviewed: Minor edits. Submitted to ITAC/ISAC Review Timeframe 9/7/17 to 10/2/17 |
| 10/2/2017 | E. Hudson | Reviewed and Approved |
| 5/14/2020 | E. Hudson | Reviewed and Approved |