# Cloud Computing

## Division:

Administration and Finance

## Department:

Information Technology Services

## Contact Information:

Nish Malik / Associate Vice President and Chief Information Officer / (415) 405-4105 / nish@sfsu.edu

## Effective Date:

Wednesday, February 1, 2017

## Revised Date:

Friday, May 14, 2021

## Authority:

ICSUAM 8040 - Managing Third Parties

ICSUAM 8060 - Access Control

ICSUAM 8065 - Asset Management

ISO/IEC 27017:2015 Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services

## Objective:

The purpose of this practice directive is to establish a standard that defines campus practices for the assessment, procurement, security, and operation of cloud computing services used for instruction, research, and administrative purposes.

***Definitions***

**Appropriate Administrative Authority**: Defined as associate vice president, vice president, dean, director, department, or program chair

**Cloud Computing Service:** The utilization of servers or information technology services of any type that are not hosted by the CSU or auxiliaries including, but not limited to, social networking platforms, applications, file storage, infrastructure, and content hosting.

**Large Amounts of Level 2 Data:** Generally defined as Level 2 data elements that represent a collection of records from one third or more of a campus group or population; for example: student names with birth dates for over 10,000 student records, or employee names and personal email addresses for over 2,000 employee HR records would be categorized as large amounts of Level 2 data.

## Statement:

The purpose of this practice directive is to ensure that CSU data is not inappropriately stored or shared using cloud computing services. Note that all requirements from all other relevant CSU policies and standards remain in full effect when cloud computing services are used.

## Scope

This practice directive applies to all uses of Cloud Computing Services by the SF State and its auxiliaries. The practice directive applies regardless of the method of acquisition and includes purchase orders, procurement cards, petty cash, and services provided free of cost, as a pilot, or proof of concept.

## Acquisition Review

### Technology acquisition review (TAR)

All cloud computing service acquisitions must complete a Technology Acquisition Review (TAR) before they are purchased or deployed. This applies to new acquisitions, software upgrades, deployment scope changes, and renewals. The technology acquisition review form should be completed by an individual with knowledge of planned use. Any purchase or acquisition without an approved TAR is considered an unauthorized purchase. TAR's submitted after a purchase/acquisition require approval from the appropriate administrative authority.

For cloud computing services that store or access SF State level 1 data or large amounts of level 2 data, the vendor must provide a HECVAT, a security audit report or a security controls certification as part of the TAR process.

For more information on the TAR process, please see the Technology Acquisition Review page.

### Inventory of Cloud Computing Services

The data collected from the technology acquisition review process will also be used to create an inventory of cloud computing services that will be made available to campus stakeholders. Cloud computing services acquired as campus standards will be clearly identified.

### Campus Cloud Service Standards

SF State will evaluate and select campus-wide cloud-based solutions to meet the needs of the organization. These will be identified as standard campus cloud services.

The selection criteria includes:

- Enterprise-grade security and data privacy
- University data ownership and management model
- University protected data must be stored in U.S. data centers
- Ability to influence product features for the benefit the SF State campus
- Vendor solution must demonstrate commitment to delivering an accessible alternative
- Compatibility with SF State's authentication system (SSO)

Standard campus cloud services provide cost savings to the campus by reducing the number of products that need to be acquired, supported, and assessed for accessibility and information security compliance.

Departments wishing to acquire alternative solutions to standard campus cloud services must document why the campus solution cannot be used and receive approval from the information security and accessibility teams before acquiring the technology. Risk Acceptance requests can be made using the Technology Acquisition Review Request form.

## Access Control

### 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

Whenever possible, cloud services must use a campus central authentication method in order to ensure that campuses may appropriately provision and de-provision identities and authorization for campus personnel. 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. SF State uses Shibboleth for single-sign-on because it ensures the cloud provider does not access SF State passwords.

### When Central Authentication is Impractical

Where campus authentication is impractical for cloud services the campus must have a way to recover any account when the community member separates, such as using a campus e-mail 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. All passwords must meet SF State's complexity standards.

### 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), SF State central authentication or comparable SF State multi-factor authentication is required for any service storing or accessing SF State level 1 data.

### Authorization

The individual(s) responsible for managing user access levels and roles must be identified and the task included in their position description.

When technically feasible, Shibboleth attributes and/or active directory security groups should be used to manage user access control.

## Sensitive Data

### 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.

### Protected level one data stored in the cloud

SF State shall not use cloud computing services to store protected level 1 data unless such access can be limited by contractual, technical or procedural controls in order to reduce inadvertent exposure and remedy potential loss.  Examples of adequate controls include but are not limited to:

- Periodic reports showing permissions/access granted to "outside" identities
- Configuration options which limit user ability to share documents or folders outside the organization
- Data is not stored or transmitted outside of the US
- Training and awareness for users who access and store protected level one data
- Periodic assessment of protected level one data stored off campus
- Accurate records of all data stored in cloud
- Including CSU IT Supplemental Provisions in the contract

### Safety of data

Protected Level 1 and 2 data (including credentials) stored in the cloud (including test and development environments, backups and data warehouses) must be encrypted both at rest and in transit.

Encryption keys must be held by the campus unless vendor has appropriate key management in place.

### 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.

## Implementation

Responsibility for implementing this Practice Directive will rest with Information Technology Services and Information Technology (IT) departments across campus. Submit any apparent violation of Cloud Computing Practice Directive to the appropriate administrative authority or to service@sfsu.edu.

## Non-Compliance

Non-compliance with applicable policies and/or practices may result in suspension of procurement, network and systems access privileges. In addition, disciplinary action may be applicable under other University policies, guidelines, implementing procedures, or collective bargaining agreements

## Searchable Words:

cloud, computing, compliance, security, accessibility