

INTRODUCTION

Cloud computing services are application, platform and infrastructure resources that are accessed through the Internet. Infrastructure services hosted and contractually provided by companies such as Apple, Google, Microsoft®, and Amazon, enable the campus to leverage powerful computing resources which offer an array of operational options that would otherwise be beyond the campus means to purchase and support.

Cloud services provide a wide range of business activities, supporting communication, which includes; collaboration; project management; scheduling; data analysis, processing, sharing, and storage. Cloud computing services are generally easy for organizations to use, they are accessible over the Internet through a variety of platforms (workstations, laptops, tablets, and smart phones), and they may be able to accommodate spikes in demand much more readily and efficiently than in-house computing services.

Cloud computing is a kind of Internet-based computing that provides shared processing resources and data to computers and other devices on demand. It is a model for enabling ubiquitous, on-demand access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services),^{[1][2]} which can be rapidly provisioned and released with minimal management effort. Cloud computing and storage solutions provide users and enterprises with various capabilities to store and process their data in third-party [data centers](#).^[3] It relies on sharing of resources to achieve coherence and [economy of scale](#), similar to a utility (like the [electricity grid](#)) over a network.

(From Wikipedia, the free encyclopedia)

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:

- 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

PURPOSE

The purpose of this standard is to align with current or emerging CSU Cloud policy and to ensure that CSU sensitive data is not inappropriately stored or shared using public cloud computing and/or file sharing services. Cloud computing and file sharing, for this purpose, is defined as the utilization of servers or information technology hosting of any kind that is not controlled by, or associated with, CSU or campus for services such as, but not limited to, social networking applications (i.e. blogs and wikis), file storage (Dropbox), and content hosting (publishers text book add-ons). A list of acceptable and unacceptable cloud services is in the appendix at the end of this policy.

There are three primary categories of cloud computing which require campus consideration.

- Use of Software-as-a -Service including but not limited to Dropbox, Google Apps for Education, Microsoft Office 365.
- Platform and Infrastructure-as-a-Service including but not limited to Amazon Web Services (AWS) and Microsoft Azure.
- Security and Contract Review

SCOPE

This standard applies to the following:

- Central and departmentally-managed campus information assets.
- All users employed by campuses or any other person with access to campus information assets.
- All categories of information, regardless of the medium in which the information is held or transmitted (e.g. physical or electronic).
- Information technology facilities, applications, hardware systems, and network resources owned or managed by the CSU.
- Auxiliaries, external businesses and organizations that use campus information assets must operate those assets in conformity with the CSU Information Security Policy.

POLICY Use of Software-as-a-Service

1.1 Definition

Software as Service Environments: *Cloud 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 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.

This standard endorses the use of cloud services for file storing and sharing with vendors who can provide appropriate levels of protection and recovery for University information, and with explicit restrictions on storage of University Level 1 Protected and Level 2 Private Information. While cloud storage of files can expedite collaboration and sharing of information anytime, anywhere, and with anyone, there are some guidelines that should be in place for the kind and type of university information that is appropriate for storing and sharing using these services. Even with personal use, one should be aware of the level of protection available for your data using such a cloud service.


1.2 Standard for Use of Cloud Services for Storage, Communication, and Productivity Involving University Data (Software as a Service)

- 1.2.1 Use of cloud services for storage, communication and productivity involving University Level 1 data is **prohibited**. Examples include but are not limited to Dropbox, Google Apps for Education, Office 365, and Exchange Online.
- 1.2.2 Use of cloud services for storage of University Level 2 data must be limited to services contracted by and supported by the University. Cloud services which are not supported by and provisioned by the University are prohibited.


Most cloud services, such as Google Docs, make it easy for individuals to sign-up and use (self-provision) their services via an end user license agreement (EULA), often at no monetary cost. However, CSU and campus faculty/staff, must be very cautious about self-provisioning a cloud service to process, share, store, or otherwise manage institutional data (as defined by the CSU Data Classification Standard). Self-provisioned cloud services may present significant data management risks or are subject to changes in risk with or without notice. Virtually all cloud services require individual users to accept click-through agreements. These agreements do not allow users to negotiate terms, do not provide the opportunity to clarify terms, often provide vague descriptions of services and safeguards, and often change without notice.

- 1.2.3 Use of cloud service offerings that are not supported, provisioned and contracted by the University for storage, communication, and productivity involving University records including vital records which are classified as public or Level 3 data is not recommended. University data should be limited to University supported and provisioned services.
- 1.2.4 The use of public cloud services for academic, non-FERPA data is permitted.


1.3 The following outlines the data classification and proper handling of CSU data.

 **Use Prohibited** *Use Prohibited* Use of this service with the regulated data type is prohibited. Do not use this service to send, store or share the regulated data type.

- a) Disclosure exemptions - Information maintained by the University that is exempt from disclosure under the provisions of the California Public Records Act or other applicable state or federal laws.
- b) Severe risk - Information whose unauthorized use, access, disclosure, acquisition, modification, loss, or deletion could result in severe damage to the CSU, its students, employees, or customers. Financial loss, damage to the CSU's reputation, and legal action could occur.
- c) Limited use - Information intended solely for use within the CSU and limited to those with a "business need-to know."
- d) Legal Obligations - Information for which disclosure to persons outside of the University is governed by specific standards and controls designed to protect the information.

 **Use Restricted** *Use Restricted* Use of this service with the regulated data type is restricted and approval is required.

- a) Sensitivity - Information which must be protected due to proprietary, ethical, contractual or privacy considerations.
- b) Moderate risk - Information which may not be specifically protected by statute, regulations, or other legal obligations or mandates but for which unauthorized use, access, disclosure, acquisition, modification, loss, or deletion of could cause financial loss, damage to the CSU's reputation, violate an individual's privacy rights, or make legal action necessary.

 **Use Permitted** *Use Permitted* No technical, policy, or contractual issues exist that prohibit use of this data type with this service. You may send, store or share the regulated data type with this service if your data steward and your department/unit policies permit you to do so.

- a) Information which may be designated by your campus as publically available and/or intended to be provided to the public.
- b) Information at this level requires no specific protective measures but may be subject to appropriate review or disclosure procedures at the discretion of the campus in order to mitigate potential risks.

- c) Disclosure of this information does not expose the CSU to financial loss or jeopardize the security of the CSU's information assets.












How to Identify

CSU Protected Levels of Data

(PL-1, PL-2 and PL-3)







Example of Types of CSU Defined Data

****Not Exhaustive**

FERPA <i>Name with:</i>	HIPAA <i>Name with:</i>	PII <i>Name with:</i>	GLBA <i>Name with:</i>	CREDIT CARD	Law Enforcement Records <i>Name with:</i>	Campus Access Credentials	Campus Financials
Grades DOB Photo Advising PL2 	Health Records or Insurance Records PL1 	Personally Identifiable Information (SSN) (Passport) (Visa) PL1 	Financial Information (Bank Accounts) (Tax Returns) PL1 	Payment Card Information PL1 	Driver's License Criminal Background PL1 	Account And Password PL1 	 PL2 
Campus Attorney client communications PL2 	Employee Information <i>Name with:</i> (Home Address) (Home Phone) (Personal Email) (Marital Status) (Gender) (Evaluation) (Personnel Actions) PL2 	General Information publically available Publications Web PL3 					

IT Tools to Send, Store, Transmit or Share CSU Protected Data

	CSU Protected Level 1	CSU Protected Level 2	CSU Protected Level 3
Calendar			
Google			
Outlook – Internal			
Outlook – External			
Collaboration Services			
Blogs			
Google Docs			
DropBox – Personal			
DropBox - Department			
DropBox - Business			
OneDrive – Personal			
One Drive - Business			
Office 365 SharePoint			
Box			
Code42			
Office 365			
Email			
Gmail			
Outlook Internal Email			
Outlook External Email			
Yahoo			
HelpDesk Ticketing			
Service-Now			
Managed Servers			
Campus SharePoint			
Campus SAN Storage			
Campus SharePoint (Web)			
Survey Tools			
Qualtrics			
Web & Video Conferencing			
Office 365 Skype Online (Video)			
Office 365 Online (IM)			
Web Conferencing (Zoom)			
Video Conferencing			
Learning Management			

SkillPort			
	CSU Protected Level 1	CSU Protected Level 2	CSU Protected Level 3
Moodle			

POLICY Platform-as-a-Service and Infrastructure-as-a-Service

1.4 Definition

Platform as a Service Environments: The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages 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 application hosting environment configurations.

Infrastructure as a Service Environments: 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, deployed applications; and possibly limited control of select networking components (e.g., host firewalls).

1.5 Policy for Use of Cloud Computing Services (Platform as a Service)

It is essential that security, privacy, and other IT management requirements have been adequately addressed prior to the use of Cloud Computing services.

- 1.5.1 Use of Cloud Computing Platform as a service environment must be formally authorized in writing by The Information Security Officer and the Director of Contracts and Procurement through the IT Procurement Review Process.
- 1.5.2 Platform as a Service environments require security related risk assessments such as SSAE-16 and Cloud Security Alliance (CSA) STAR Certification.
- 1.5.3 Vendors providing or utilizing Cloud Computing Platform as a Service to provide services involving University Level 1 or Level 2 data must agree to appropriate terms and conditions found in the attached documents "IT Procurement General Provisions" and "IT Supplemental Provisions for Acquisitions".

1.6 Policy for Use of Cloud Computing Services (Infrastructure as a Service)

It is essential that security, privacy, and other IT management requirements have been adequately addressed prior to the use of Cloud Computing services.

- 1.6.1 Use of Cloud Computing Platform as a service environment must be formally authorized in writing by The Information Security Officer and the Director of Contracts and Procurement through the IT Procurement Review Process.
- 1.6.2 Platform as a Service environments require security related risk assessments such as SSAE-16 and Cloud Security Alliance (CSA) STAR Certification.
- 1.6.3 Vendors who provide or utilizing Cloud Computing Platform as a Service to provide services involving University Level 1 or Level 2 data must agree to appropriate terms and conditions found in the CSU IT Procurement and the Supplemental Provisions.

1.7 **Compliance with Legal and Regulatory Requirements:**

- 1.7.1 Cloud computing services must comply with appropriate laws and regulations, including but not limited to the Family Educational Rights and Privacy Act of 1974 (FERPA), the Health Insurance Portability and Accountability Act (HIPAA), and the Gramm-Leach-Bliley Act (GLBA).
- 1.7.2 Cloud-computing services that use, store, or process University data must comply with CSU and campus Information Security Policies and Standards.

2.0 **Exit Strategy:**

Cloud services should not be engaged without developing an exit strategy for disengaging from the vendor or service and integrating the service into business continuity and disaster recovery plans. The University must determine how data would be recovered from the vendor.

2.1.1 Approved cloud services must:

- Comply with all current laws, CSU and campus Information Security Policies and Standards, and risk management policies.
- Use of Cloud Computing services must comply with relevant privacy laws and regulations, and appropriate language must be included in the contract language accepted by the vendor. Campus roles and responsibilities for Cloud Computing privacy requirements must be defined.
- All use of Cloud Computing services must be approved in writing through the IT Procurement Review (ITPR) Process.

- The Cloud computing service may not be put into production use until contracts and agreements are approved and finalized by the Director of Contracts and Procurement.

3.0 Procurement of Cloud Services

The University should consider the following contract terms to ensure a minimum level of information security protection:

- Data transmission and encryption requirements
- Authentication and authorization mechanisms
- Intrusion detection and prevention mechanisms
- Logging and log review requirements
- Security scan and audit requirements
- Security training and awareness requirements

- 3.1 All Contracts and services involving University data, Level 1 Protected, or Level 2 Private data must be approved through the IT Procurement Review (ITPR) Process.
- 3.2 Data Owners of University data must authorize the use of cloud services where Level 1 and Level 2 data are involved.
- 3.3 Monitor changes to the service's safeguards
- 3.4 Have a clearly designated Information Manager for the institutional data. Defined by the Information Roles and Responsibilities Policy, the Information Manager is the individual charged "to ensure the responsible management and use of institutional data."
- 3.5 Know the retention period and, when applicable, the destruction date of the institutional data. Retention periods are often defined by the general Records Retention Schedule (<http://www.calstate.edu/recordsretention/>) or other records policies.
- 3.6 When appropriate, destroy the institutional data securely.
- 3.7 Using Cloud Computing Services: Faculty, staff, and students may not self-provision cloud services to store, process, share, or manage Level 1 Protected Data. Defined by the CSU Data Classification and Protection Standards.

Appendix A: Definitions:

General Data Protection Terms:

The University must specify particular data protection terms in a contract with a cloud-computing vendor. In this way, the University creates a minimum level of security for University data. A minimum level of security ensures that the University data is kept confidential, is not changed inappropriately, and is available to the University as needed.

General Cloud Environments:

Software as a Service: *Cloud Software as a Service (SaaS).* The capability provided to the campus user to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a Web browser (e.g., Web-based email), or a program interface. The campus user 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.

Platform as a Service Environments: The capability provided to the campus user is to deploy onto the cloud infrastructure campus user -created or -acquired applications created using programming languages and tools supported by the provider.³ The campus user 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 application hosting environment configurations.

Infrastructure as a Service Environments: The capability provided to the campus user 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, deployed applications; and possibly limited control of select networking components (e.g., host firewalls).

Private cloud: The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple campus users (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.

Community cloud: The cloud infrastructure is provisioned for exclusive use by a specific community of campus users from campus areas that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the campus areas, a third party, or some combination of them, and it may exist on or off premises.

Public cloud: The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of above. It exists on the premises of the cloud provider.

Hybrid cloud: The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds)."

University data: University data covers any item of information that is collected, maintained, and used by the University for the purpose of carrying out the business of the University, subject to or limited by any overriding contractual or statutory regulations. University data may be stored either digitally or on paper and may take many forms, including, but not limited to, text, graphics, images, sound, and video. Research data, scholarly work by faculty or students, and intellectual property that does not contain personally identifiable information or other data protected by law or University policy is not considered University data, nor is an individual's own personally identifiable information (PII) unless it's used as described above. University data must be available to the University and other individuals as required under University policies and is subject to CSU Policy & Standards, CSU Data Classification, and other appropriate controls depending on the sensitivity of the data.

Related Documents:

CSU Responsible Use Policy

CSU Classification and Protection Standard

CSU Records Retention Policy EO 1031

CSU General Provisions for IT Procurement

CSU Supplemental Provisions

For more details about cloud computing see “The [NIST Definition of Cloud Computing](#) (link is external).”

Documentation Review & Approval

Review / Approval History

Review Date	Reviewed By	Action (Reviewed, Recommended or Approved)
11/30/2016	Kerry Boyer	Reviewed and approved