CALIFORNIA STATE UNIVERSITY
BAKERSFIELD

Cloud Computing Policy

CSU Bakersfield Policy

Document Number:	ITS-90.002	**Last Revision Date:**	6/9/2022
Responsible Office:	Information Technology Services	**Effective Date:**	7/1/2018
Primary Author:	CIO & AVP of Information Technology		

General Description

Purpose:

This policy is intended to manage cloud computing services that can storage and manage California State University Bakersfield's data. These cloud services must be managed and maintained in a manner to properly protect the campus's data.

Definition:

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 Auxiliaries, such as personal cloud accounts."
CSU Information Security Policy and Standards - Section 8 Cloud Storage and Services

Scope:

This policy applies to the following:

- All campus departments – whether auxiliaries or state side.
- All employees, students, consultants, vendors, or persons of interest that have access to data.
- All cloud services such as:
    - SaaS – Software as a Service
    - PaaS – Platform as a Service
    - IaaS – Infrastructure as a Service
    - DaaS – Data as a Service
- Classification Description:
    - CSU Level One Data – "Confidential" – examples: Social Security Number with Name, Medical Records, Bank Account or debit/credit cards with security or access codes.

- CSU Level Two Data – "Internal Use" – Student Information – educational records, trade secrets or intellectual property, employee information such as – net salary, home address, gender.
- CSU level Three Data – "General" – Information identified as publicly available. Such as email address, First and Last Name.

Policy/Procedure

1. Storing or transmitting of level 1 data as defined CSU Information Security Policy Data Clasification Levels by is prohibited on all cloud services unless:
a. Contracted through the ITS-Solutions Consulting group
b. A contract with vendor contains appropriate Information Security Supplemental Language
c. Utilization of the service is approved by the appropriate data owner
d. Approval is granted by the Information Security Office and approved by the President or Vice President
e. The cloud service must be configured to utilize the campus multi-factor service Duo or other approved multi factor solution. In accordance to CSU Information Security Policy - Section 8. Cloud Storage and Services.

2. Storing or transmitting of level 2 data as defined by CSU Information Security Policy Data Clasification Levels is prohibited on all cloud services unless:
a. Contracted through the ITS-Solutions Consulting group
b. A contract with vendor contains appropriate Information Security Supplemental Language
c. Utilization of the service is approved by the appropriate data owner
d. Approval is granted by the Information Security Office and approved by the President or Vice President
e. The cloud service must be configured to utilize the campus multi-factor service Duo or other approved multi factor solution. In accordance to In accordance to CSU Information Security Policy - Section 8. Cloud Storage and Services.

3. Cloud application administrators are responsible for maintaining accurate and timely user account status
a. Terminated users must have their account to the cloud service disabled no later than the day of termination.
b. Accounts should be provisioned with the Principle of Least Privilege

4. Cloud application administrators are responsible for reviewing all accounts and their associated level of application access on a quarterly basis
a. Active accounts should be compared to employee records. Any terminated users should have their accounts removed or disabled.

5. Cloud application administrators are required to provide an annual report of compliance with this

policy.
a. Once a year on November 1st any administrator of a cloud-based SaaS application will be required to provide a listing showing all the accounts and their associated rights or privilege level associated to that account to the Information Security Officer (ISO). More information about this process can be found in the Cloud Audit procedures document.
b. Application Owners of applications that manage Level one data must work with the cloud application vendor to get the updated SOC 2 audit and cyber liability insurance certificate of insurance (COI) on an annual basis and post those documents with the Information Security Officer (ISO)no later than November 1st of every year.

Failure to maintain these reporting requirements will lead to the violating application being blocked from running on the campus network.

Matrix of cloud services

Below is an excerpt from our approved list of cloud services. The entire list can be found within CSUB Approved Cloud Services document. If you see a "No" then having that level of data within that service is prohibited.

Examples of CSUB Approved Cloud Services

Solution	CSU Level One Data	CSU Level Two Data	CSU Level Three Data
Office 365 Email	No	Yes	Yes
Office 365 OneDrive	No	Yes	Yes
Office 365 Sharepoint	No	Yes	Yes
Groups/Team	No	Yes	Yes
Box	No	Yes	Yes
Secure Box **	Yes	Yes	Yes
Zoom	No	No	Yes
Qualtrics	No	No	Yes
Learning Management System	No	Yes	Yes

** The following services must be configured by ITS specifically for you.

Note: Please see CSUB Approved-Not Approved Cloud Service document for full list.

Examples of Cloud Services not contracted by CSUB

Solution	CSU Level One Data	CSU Level Two Data	CSU Level Three Data
Dropbox	No	No	Yes
Google Mail	No	No	Yes
Yahoo Mail	No	No	Yes

Note: Please see CSUB Approved-Not Approved Cloud Service document for full list.

Review (Frequency and Process)

This policy shall be reviewed every two years by the Associate Vice President & CIO or a designate and provided to the Vice President Business and Administrative Services for approval and then to Cabinet for final approval.

Related Documents

Related Content:

CSU Information Security Policy - Data Classification Levels
CSU Information Security Policy - Cloud Storage and Services