



Origination	12/2024
Last Approved	12/2024
Effective	12/2024
Last Revised	12/2024
Next Review	12/2034

Chapter Lead	Nohemy Ornelas: Chapter 3(CC),4&5
Policy Area	Chapter 3 General Institution
References	Non CCLC

AP 3736 Information Security Cloud Storage

1. PURPOSE AND SCOPE

The objective of this Administrative Procedure is to provide the framework within which San Bernardino Community College District (SBCCD) employees can create, store, share, and process data in “cloud storage” environments.

This is one of a series of information security Administrative Procedures maintained by the District Information Technology (IT) Department with collaboration and input from the colleges and designed to protect district information systems.

Please refer to AP 3725: Information Security Program Overview for applicability to staff and external parties and to AP 3726: Information Security—Data Classification for detailed information about the types of data.

2. CLOUD STORAGE

- a. Cloud Storage: A model of networked online storage where data is stored in virtualized storage pools not contained within the device through which the data is accessed. Such data storage is most often offsite and usually managed by independent vendors (e.g., Google Drive or G-Suite, Apple iCloud, Microsoft OneDrive). Cloud storage of data classified as Internal or Restricted can exist within the district-approved Learning Management System (such as Canvas), or district-approved cloud storage (such as Sharepoint or OneDrive).
- b. Data Types: Per AP 3725 and AP 3726, district data is classified in the following categories:
 - i. Public: information made for public distribution (such as press releases, public web pages, or publicly available data;
 - ii. Internal: data that must be protected due to proprietary or business

reasons but is not personally identifiable or sensitive;

- iii. Restricted: information that is sensitive in nature, may be protected by statute, regulation, or contractual requirements, and can include personally identifiable information like student data and grades, credit card data, human resources information, or health-care related information III.

3. APPROPRIATE USE OF CLOUD STORAGE

While recognized as a valuable teaching and productivity tool, cloud storage increases the risk of a data breach. As a result, users must adhere to the following requirements:

- a. SBCCD employees have a responsibility to protect the college and District data, particularly confidential data about individuals.
- b. Internal and Restricted district data may be stored by employees on cloud storage under the following conditions:
 - i. The cloud storage must be District-approved cloud storage.
 - ii. Access to the data in cloud storage is secure (e.g., requires password and/or dual factor authentication for access).
 - iii. Devices (including desktop, notebook or tablet computers and cellular phones) through which the cloud storage is accessed must have active password or equivalent protection.
 - iv. Networks (including home Ethernet or wireless networks) through which the cloud storage is accessed must be encrypted, and have active password protection.
 - v. Employees may not access cloud storage containing internal or restricted data through open, public or unencrypted networks (e.g., Starbucks Wi-Fi access) unless the data communication protocol is encrypted (e.g., sites beginning with https).
- c. District cloud storage will not normally be used for personal data (such as non-work documents, personal photos, or videos), although incidental and/or temporary use may be permitted. Users should be aware that any and all data transmitted or stored using District resources is subject to review by appropriate District personnel.
- d. When using cloud storage for collaboration with others, users shall grant access only to files or folders that are required for the collaboration to take place only for the duration of the collaboration, removing permissions in a timely manner when the collaboration has concluded.
- e. The Vice Chancellor of Educational & Student Support Services or designee is authorized to make exceptions to this Administrative Procedure. Users must contact District IT or college Technology Departments to make an exception request.

4. ADDITIONAL INFORMATION

- a. Employees may contact District IT or college Technology Departments for further guidance on:
 - i. Use of cloud storage consistent with the intent of this Administrative

Procedure;

- ii. Rights and permissions requested by a cloud storage application prior to installation to ensure they do not put SBCCD data or systems at risk of being compromised;
 - iii. Methods of secure access to cloud storage;
 - iv. Designation of data types, and appropriate ways to store that data.
- b. The district will provide support and opportunities for users faculty, staff, and students to familiarize themselves with the security requirements of the data in their custody to make appropriate, informed decisions about data storage.
 - c. District IT and college Technology Services provide technical support only for approved cloud storage (see appropriate technology website for a list of approved cloud storage), LMS, and cloud storage clients or apps, and not personal/public storage such as Dropbox and Box.com.

References:

NIST SP 800-53 Rev. 4 AC-2, AU-12, CA-7, CM-3, CM-8, SC-5, PE-3, PE-6, PE-20, SC-7, SI-4;
HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(ii)(D), 164.308(a)(5)(ii)(B), 164.308(a)(5)(ii)(C),
164.308(a)(8), 164.310(a)(1), 164.310(a)(2)(ii), 164.310(a)(2)(iii), 164.310(b), 164.310(c), 164.310(d)(1),
164.310(d)(2)(iii), 164.312(b), 164.312(e)(2)(i), 164.314(b)(2)(i)

Approval Signatures

Step Description

Approver

Date

Approved per Level 2 process
in AP 2410

Kelly Goodrich: PPAC Support

12/2024