ADMINISTRATIVE REGULATION 3736

SOUTH ORANGE COUNTY COMMUNITY COLLEGE DISTRICT

GENERAL ADMINISTRATION

INFORMATION SECURITY- CLOUD STORAGE

I. PURPOSE AND SCOPE

The objective of this Administrative Regulation is to provide the framework within which South Orange County Community College District (SOCCCD) employees can create, store, share, and process data in "cloud storage" environments.

This is one of a series of information security Administrative Regulations 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 AR 3725: Information Security Program Overview for applicability to staff and external parties, and to AR 3726: Information Security—Data Classification for detailed information about the types of data.

II. 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 Gauchobox or the district's instance of G-Suite).

B. Data Types: Per AR 3725 and AR 3726, district data is classified in the following categories:

1. Public: information made for public distribution, (such as press releases, public web pages, or publicly available data;
2. Internal: data that must be protected due to proprietary or business reasons, but is not personally identifiable or sensitive;
3. 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. 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. All SOCCCD 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:

   1. The cloud storage must be District-approved cloud storage as posted in the appropriate technology department website.

   2. Access to the data in cloud storage is secure (e.g., requires password and/or dual factor authentication for access).

   3. Devices (including desktop, notebook or tablet computers and cellular phones) through which the cloud storage is accessed must have active password or equivalent protection.

   4. Networks (including home Ethernet or wireless networks) through which the cloud storage is accessed must be encrypted, and have active password protection.

   5. 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. Employees should back up all district data to a secure physical device, and not store the data only in cloud or hosted storage.

F. The Vice Chancellor of Technology and Learning Services or designee is authorized to make exceptions to this Administrative Regulation. Users must contact District IT or college Technology Departments to make an exception request.

IV. ADDITIONAL INFORMATION

A. Employees may contact District IT or college Technology Departments for further guidance on:

   1. Use of cloud storage consistent with the intent of this Administrative Regulation;

   2. Rights and permissions requested by a cloud storage application prior to installation to ensure they do not put SOCCCD data or systems at risk of being compromised;

   3. Methods of secure access to cloud storage;

   4. Designation of data types, and appropriate ways to store that data.

B. The district will provide opportunities for users 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)