UCSB Guidelines for Cloud Use and Storage

GENERAL

This document establishes guidelines governing appropriate use of personal cloud applications for end users at the University of California, Santa Barbara. These guidelines recognize the power of cloud platforms for productivity and collaboration. However, all users must also understand their responsibilities surrounding protected data/information and the privacy of students.

Please note that these guidelines apply to personal cloud accounts and cloud services or instances that are not subject to University contract. Different rules may apply for University-contracted services, and users should consult the appropriate documentation or the IT body providing that service for specific guidance. As a general rule, University-contracted services are those that require your University netID and password to log in. More guidance on the use of University-contracted services can be found at http://www.security.ucsb.edu/faculty-staff/cloud-services.

Whenever possible, work-related information and documentation should be stored using University-contracted services and your University account (login with netID and password). It is recognized, however, that at times staff may require the use of personal cloud accounts in order to perform their work (e.g. when collaborating with staff from another campus when there is no common tool, or in situations where there is no University-contracted tool available to perform a particular service). Given the differing levels of security of cloud platforms, it is imperative that all staff understand the security classifications of data/information and the appropriate use of storing or sharing data/information on personal cloud applications or using personal accounts.

DEFINITION

Cloud Application: any of several, often proprietary, parts of the Internet that allow online processing and storage of documents and data as well as electronic access to software and other resources (e.g. Dropbox, Google Drive, etc.)

UNIVERSITY BUSINESS USE

Staff using cloud platforms shall:

- be aware of data classification protection levels 1, 2 and 3 (below).
- agree never to store or share data classified at protection levels 1, 2 and 3 in personal cloud applications or accounts.
- not share files with those who do not have a business requirement to access them.
- understand that not all cloud platforms are supported by all Help Desks.
- upon ending employment, return or permanently delete university-related information or resources.
- when in doubt, always err on the side of protecting student data and other sensitive information.

Data Classification & Security Protection Levels

Data Class Protection Level	Adverse Business Impact	Data Types	Cloud Storage
3	Extreme	Usernames and passwords.	No
2	High	California state law "notice-triggering data" (e.g. SSN, credit card information, HIPAA data).	No
1	Moderate	Personal information (unless otherwise classified as Level 0, 2 or 3), including FERPA-protected student data, and personnel records. Data protected by contract, depending on terms of agreement (e.g. license software, license software keys, and library paid subscription electronic resources).	No
0	Limited or None	Policy information, data intended for public consumption (e.g. Admissions PPTs, general campus stats, etc.), student data specified under UC policy as "directory" information (see list at https://registrar.sa.ucsb.edu/recinfo.aspx#DirectInfo).	Yes

TRAINING

All staff should familiarize themselves with the data security classifications above. In addition, staff working with student data of any kind must complete the campus FERPA training at https://my.sa.ucsb.edu/ferpatraining/login.aspx. Staff working with medical data should also complete the campus HIPAA training at https://www.learningcenter.ucsb.edu/ (search for "HIPAA").

RESOURCES

University of California Electronic Communications Policy: http://www.ucop.edu/ucophome/policies/ec/
UCSB Interim Electronic Communications Implementing Guidelines 5612:
http://www.policy.ucsb.edu/policies/policy-docs/ecp.pdf
UCSB online FERPA training: https://my.sa.ucsb.edu/ferpatraining/login.aspx

Revised 11/10/2016