Division of Student Affairs Guidelines for Cloud Storage

GENERAL

This document establishes guidelines governing the use of cloud storage for all employees of the Division of Student Affairs at the University of California, Santa Barbara. These guidelines recognize the power of third-party or "cloud" storage as a useful productivity and collaborative tool. It was also written to remind all Division users of the importance of protected classes of data and the important duty we have to protect the privacy of our students.

The Division of Student Affairs supports the sharing of data among divisional staff on the divisionally supported drives (such as the J and K drives) that users can access via remote log-in. Remote access should be the first-choice for all users wishing to access files remotely as it is supported and secure. Anyone wishing to use remote access should request it from the SIS&T Help Desk. The Division recognizes that staff, at times, may require the use of cloud storage platforms in order to perform their work with those outside the division. Given the differing levels of security on cloud platforms, it is imperative that all Division staff be trained about the security classifications of data and the appropriate use of data on cloud platforms. The Division allows (but does not support) the appropriate use of cloud storage such as Dropbox, Google Apps and Microsoft Skydrive.

UNIVERSITY BUSINESS USE

Staff using cloud storage platforms will

- be aware of data classification protection levels 1,2 and 3.
- agree to never store data classified at protection levels 1, 2 and 3 on a cloud storage device.
- not share files with those who do not have a business requirement to access them.
- upon leaving employment in the Division the employee will return or permanently delete university-related information resources.

TRAINING

All divisional staff will undergo training covering types of data and the security classifications related to each. The training will also cover the responsibilities of end-users and best practices. (See Appendix A for a sample of data-types and their security classification.)

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