Cloud Storage Guidance

(e.g., OneDrive, Dropbox, iCloud, etc.)

Cloud storage provides Web based access to your online file storage, file sharing, and file synchronization. For purposes of this guidance, we will refer to all of these services as *'cloud storage'*. Below is guidance about using cloud storage services here at Stanislaus State.

1. The responsibility for storing Stanislaus State documents and files resides with the person who stores the data. Personal judgment is required about how and where Stanislaus State data can and should be stored.

2. Refer to the Stanislaus State Information Classification and Handling Standard for specific information about how to handle specific types of documents you may have available to you.

3. The risks to Stanislaus State are identified in the Stanislaus State Information Classification and Handling Standard, and are specified for each type or classification of data. Different data has different regulations, laws, agreements and rules, requiring protection of that data and reporting when that data is released to unauthorized individuals.

   Some examples: If you're working with grades and student's academic records, there are federal laws (FERPA). If you're working with health care information, there are federal laws (HIPAA). If you're working with SSN, there are federal and state laws. If you're working with driver's license information there are CA laws. If you're working with credit card information there are credit card regulations (PCI). If you're working on grant sponsored research, that grant has specific rules. If you're collecting data for a book or creating intellectual property, this data may be solely yours.

4. Some questions to ask yourself as the person who wants to make a copy of or store Stanislaus State data or information in a location which is in additional to its source location, and not contained within Stanislaus State network storage.
   a) If the data is released to the public what is the risk to Stanislaus State?
   b) If the data is unavailable to you when you need it, how bad would that be?
   c) Do people depend on this data to do their job?
   d) Does the cloud storage service provider agree to protect the confidentiality of the data? (assume that they do not)
   e) Does the cloud storage service use encryption?
   f) Does the cloud storage service indicate how available the data will be?

g) Does using these services follow the Stanislaus State Information Classification and Handling Standard? Does it go against any of the standards?

5. Before moving any data or files from your computer or the network to Cloud storage, you must complete a scan of your computer using Identity Finder. Identity Finder searches your computer and files for protected Level 1 data. Follow the instructions for completing a scan prior to moving any files to Cloud storage.

6. FAQ: Is it OK to store Level 1 data on cloud storage servers?
   Response: Level 1 data may not be stored in cloud storage.

7. FAQ: Is it OK to store Level 2 data on cloud storage services?
   Response: Level 2 data is everything between level 1 and public data. The people who want to store data using cloud storage services need to review the Stanislaus State Information Classification and Handling Standard and use their judgment regarding the specific level 2 data they want to store.

8. FAQ: Outside of the above guidance, is there any language specifically prohibiting the use of cloud storage services for off-campus storage of Stanislaus State level 2 or level 3/public data?
   Response: Refer to the Stanislaus State Information Classification and Handling Standard for specific information about how to handle specific types of documents.

9. If you have any questions about a specific Cloud service, storing data in an off-site Cloud service, or anything else related to data classification please call the OIT Help Desk at ext. 3687, or email them at helpdesk@csustan.edu.