



## Cloud Archival Storage Service Purchase Agreement

This document is an agreement between the **Institute for Digital Research & Education and Stephen Abrams, California Digital Library**, to provide cloud storage services under the terms and conditions outlined below.

### Specifications under this agreement are:

**Cost** – The rate for storage under CASS is based on the amount of storage in terabytes and the length of time it is requested, 1 to 5 years. The smallest increment available under this agreement is 1 terabyte for a period of one year. Current rates are available here: <https://idre.ucla.edu/cass> Note that rates are based on each transaction and are not cumulative. That is, for example, if you buy storage based on purchasing 20TB for 1 year and subsequently add another 10TB, your second transaction will be based on the 10TB number and not the cumulative 30TB number.

This rate includes the physical storage space, infrastructure to support it, administration of the users of your storage space, hardware and software upgrades and problem fixes. This rate will remain in effect until renewed through the campus. The current rate was effective December 2013.

Note that if you are using federal funds these charges will incur overhead (currently 54% as through June 2016) as they are considered a service and not equipment, which would be exempt from overhead. See: <http://www.research.ucla.edu/ocga/sr2/idcinfo.htm#FA1> for current rates.

**Space Usage Duration** – Space will be made available to you for the number of years you have purchased. During your purchase period you will be notified of the amount of time you have available on your current purchase and ultimately when it needs to be renewed. If you decide that you will renew your purchase it can be done with no interruption in access to your storage at the then current rate. If you decide that you will not renew your purchase you will have to make arrangements to move your data off of the storage server within a maximum of 30 days. During this 30-day period your data access will be changed to read-only. IDRE personnel are available to assist you with moving your data.

**Backups** – *No backups will be done on your data unless you specifically ask for this service. Although we have made every effort possible to ensure reliability and fault-tolerance of our storage systems there is no guarantee that you will not lose your data.*

**Protecting Personal Information (PI) on the Cloud Archival Storage Service** to UCLA Policy 404 <http://www.adminpolicies.ucla.edu/app/default.aspx?&id=404> any

Personal Information (PI) data stored on the Cloud Archival Storage Service must be protected.

Personal Information is defined as "an individual's first name or first initial, and last name, in combination with any one or more of the following: (1) Social Security number, (2) driver's license number or California identification card number, (3) account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account, (4) medical information, and (5) health insurance information." To that end we need to know if you are storing any Personal Information on the Cloud Archival Storage Service. If so we strongly recommend you remove it immediately. If this is not possible then you must encrypt the data per policy guidelines. If you do decide to keep it you must inform the Director of the IDRE Research Technology Group, in writing, what kind of Personal Information you have and why you must keep it on CASS. If a security breach occurs and Personal Information is stolen AND it is not encrypted then YOU as the custodian of the data are liable for the exposure.

**Export Restricted Software** - Pursuant to federal export control regulations, certain export restricted software must be protected. Export restricted software which must be protected includes: (1) certain strong encryption software, (2) software controlled under the Department of Energy 10 CFR §810 regulations, (3) software controlled under the Department of State, International Traffic in Arms (ITAR) regulations 22 CFR §120-130. If you are storing any of the above export restricted software, we strongly recommend you remove it immediately. If you do decide to keep it, you must inform the Director of the IDRE Research Technology Group, in writing, about the export restricted software in your account. If a security breach occurs, you, as the custodian of the software, are liable for the exposure and subsequent export control regulatory violations. If you have questions about how your software is controlled under export regulations, contact Claudia Modlin, Research Policy and Compliance Coordinator at [cmodlin@research.ucla.edu](mailto:cmodlin@research.ucla.edu).

#### **UCLA Data Classification Standard**

Faculty and staff use of cloud services offered by UCLA must comply with applicable University and campus policies, notably policies relating to the protection of University data and the UC Electronic Communications Policy. This includes observing the data use requirements in the IDRE CASS Use Agreement which is based on the UCLA Data Classification Standard and University-negotiated agreements established to help safeguard information about individuals and other confidential information for which the campus is a steward. Always employ due care when processing, storing, transmitting, or communicating sensitive information. Violation of these data use requirements or other campus policies may result in disciplinary action up to and including termination.

**Notification & Information** – You or your technical lead will be notified should we encounter system problems such as power outage, network upgrades, hardware failure etc.