Exhibit F
SDSC CommVault Backup Service

This attached exhibit provides the service details, scope of work, account expiration procedures, and other terms specific to the SDSC CommVault Service portion of the Core SDSC ITSS Service agreement.

A. Term

Please refer to Section 1 of the Core SDSC ITSS Service agreement document for terms of this agreement. This exhibit may be cancelled separately per the terms provided in Section 4.4 of the Core SDSC ITSS Service agreement.

B. Scope of Work

SDSC hereby agrees to provide customer the following SDSC CommVault Backup services:

SDSC will provide access to the CommVault service, client downloads, and provide client support. SDSC will store data, selected and controlled by the customer, in SDSC's storage environment. Unless specifically requested in writing, customer is responsible for managing the size, frequency, and storage retention policies of their backup sets and related data.

C. Collection Description

C.1 The data to be stored will include:

- An estimated quantity of storage as specified in Exhibit A.
- Two copies of the data will be stored on separate physical systems within SDSC's La Jolla data center. Second copy of uploaded data is created simultaneously upon upload to the SDSC Cloud.

D. Costs and Storage Allocations

D.1 COST: See cost estimate attached as Exhibit A. This cost listed in Exhibit A is based on estimated usage as provided by the Customer. Actual costs are calculated per method defined in D.1.1 below. See applicable definitions contained in Section 3.2.

D.1.1 Total cost is the sum of the Front End Data and Back End Storage costs as explained below and estimated in Exhibit A.

- An example of the Front End Storage amount is the customer selecting to back up a total of 500GB of data from one or more systems once per month. Using an example rate of $91.67/TB/Month Front end cost, customer will incur $50 per month for Front End Storage. ($91.67 * .5TB = $45.84). This is for illustration purposes only and is not meant to provide minimum billing quantities.

- The Back End Storage is based on the total amount of Data stored in the archive. For example, if a customer elects to store each 500GB dataset for 3 months, this will result in a total of 1,500GB (1.5TB) of data stored in the archive. This is the Back End storage. Using an example rate of $32.50/TB/Month, customer will incur $48.75 per month.

D.1.2 SDSC reserves the right to review and adjust rates and will give customer Sixty days' notice in advance of adjusting any storage or service rates.

E. Failure to pay fees:

Failure to pay fees when due upon agreement initiation, renewal date, or monthly billing cycle will result in the following actions:

- If SDSC is unable to collect payment when due, Customer's account will enter unpaid status. SDSC will attempt to contact Customer using the listed Customer and notification email addresses.
- If SDSC has not received payment or other billing arrangements have not been made by the due date, the following actions will be taken:
  - After 30 Days of unpaid status: Customer's account will become read only. Customer will not be able to add any new content to the account, or create any new backup sets.
  - After 60 Days unpaid status: Customer's account will be locked and Customer will be unable to log into the system via any mechanisms. Read and write privileges are removed.
  - After 90 Days unpaid status: Customer's account will be removed and all data stored will be deleted. ***Customers are responsible for keeping a backup of their data outside of the SDSC storage systems*. Customer agrees that any account that has been unpaid for 90 days is subject to immediate termination and/or loss of data and SDSC will not be held liable for any data that has been deleted under this provision.**

F. User Responsibilities

Users of SDSC CommVault resources shall ensure that the following conditions are met:

F.1 Notify SDSC of any changes to the primary technical or business contacts through email sent to support@sdsc.edu.

F.2 Appropriate Data: Customer and End Users shall ensure that all data stored in SDSC is consistent with all policies noted in this agreement. Customer should be prepared to certify that all data stored in SDSC is directly related to the project authorized by this Service Level Agreement.

F.3 Use and Distribution of Data Stored at SDSC: ***Customer and End Users represent and warrant that (1) you or your licensors own all right, title, and interest in and to all content; (2) you have all rights in your content necessary to grant the rights contemplated by this agreement; and (3) no End User Data and/or Content violates applicable law, infringes or misappropriates the rights of any third party or otherwise violates a material term of this Agreement.*** It is illegal to distribute data or software without the approval of the owner, and such distribution is therefore considered a violation of this agreement. Violations of this agreement may result in immediate termination of services.

F.4 Data Security: Customers and End Users are responsible for the security of their data and are required to protect his or her password(s). Passwords must **never** be shared. If Customer believes any passwords have been compromised, Customer should ensure such passwords are changed immediately and inform SDSC staff about the compromise as soon as possible. Both Customer and SDSC agree to notify each respective party of any breach or disclosure of the data stored within SDSC Storage within five business days of discovery. SDSC agrees to follow industry standard security practices including but not limited to regular patching of operating systems and software maintained by SDSC, centralized audit log capture and review, personnel background checks, enforcement of separation of duties, and enforcement of the principle of "least privilege." Customer is responsible for defining any additional regulations or laws associated with the type of data stored within SDSC Storage. Such additional requirements must be documented by Customer and incorporated into this Agreement via signed amendment prior to data storage.

F.5 Sensitive Information: Unless specified in the scope of work (Section 2.), this service is not intended for open/unencrypted storage of sensitive information, e.g., PHI, PII. Customer/End User is responsible for encrypting any sensitive information ***prior*** to transfer into SDSC's storage environment and for using appropriate encryption protocols. If specified in Section 2 that PHI, PII, HIPAA, FIPS, FERPA, and any other data which falls under compliancy requirements will be stored, please refer to section F.6, storage of compliancy regulated data.

F.6 Storage of compliancy regulated data: SDSC's CommVault service is capable of encrypting archived data using AES 256 bit encryption, which is the recommended encryption option. Customer must select from three encryption key management options. Each option provides a different method for encryption key storage and management. The options include: "Via Media Password" which stores both keys within Commvault, "Via Passphrase" stores keys within CommVault but requires a passphrase during restoration only (backups remain seamless with stored keys), and "No Access" which requires that the user upload the stored key, which only the customer possesses, before any restore AND requires passphrase. SDSC will NOT store "No Access" keys or passphrases for the "Via Media require Password" option for customers. SDSC is not responsible for lost keys or passwords and *cannot* recover data if the customer is unable to provide the key or passphrase.

F.7 Privacy: SDSC will use Customer/End User Data only for the purpose of fulfilling its duties under this Agreement and for Customer's sole benefit, and will not share such Data with or disclose it to any Third Party without the prior written consent of Customer or as otherwise required by law or government regulation. By way of illustration and not of limitation, SDSC will not use such Data for SDSC's own benefit and, in particular, will not engage in "data mining" of Customer Data or communications, whether through automated or human means, except as specifically and expressly required by law or authorized in writing by Customer.

F. 8 Backups of Critical Customer Data: ***Customers and End Users are responsible for keeping a backup of their data outside of the SDSC storage systems. File systems and archival storage systems are very reliable; however, data can be lost or damaged due to media failures, hardware failures, user actions, sys admin actions pursuant to client instruction and/or mistakes, network failure, power failure, and acts of nature included but not limited to earthquakes, fires, floods, or other Natural disasters.***

Note that SDSC cannot be held responsible for errors or problems with data before its residence in SDSC storage. The process of transferring data and validating it upon arrival at SDSC is separate from actual storage of the data. Potential problems include but are not limited to instances such as bad hard drives and improper data storage, handling, and maintenance on the part of the data provider. Customer and/or End Users are responsible for running data integrity checks during transfer of data to/from SDSC storage systems to verify that stored/retrieved files are intact; Customers can check files against the MD5 checksums held in the system.

F.9 Customers, End Users, and SDSC agree to follow all applicable Federal, State, University, and SDSC policies and procedures.

F. Deliverables and cost:

See Exhibit A for deliverables and cost estimates based on customer's estimated usage.

* SDSC CommVault "front end" and "back end storage" and SDSC Cloud Storage are "On-Demand" and Customer will be billed for actual usage per section D of this exhibit.