SDSC RDS
Core Service Level Agreement

This Service Level Agreement ("Agreement"), dated July 1st, 2019 ("Agreement Effective Date"), is between the San Diego Supercomputer Center ("Service Provider") and California Digital Library – USS ("Customer"). The San Diego Supercomputer Center (SDSC) is an organized research unit within the University of California, San Diego. Service Provider and Customer may be referred to in this Agreement individually as a "Party" and together as the "Parties." Exhibit A, containing the cost estimate for this Agreement, is attached hereto and incorporated by reference herein. Exhibits D-I, containing service specific terms, deliverables, and cost details, may be attached and incorporated by reference herein.

In consideration of the mutual covenants set forth herein, the Parties agree as follows:

1. Term

The terms of this Agreement will be from July 1st, 2019 to June 30th, 2020. This Agreement may be terminated by Customer or Service Provider according to early termination of service dates as provided in section 4.4 of this Agreement.

2. Scope of Work

Service Provider hereby agrees to provide Customer one or more of the following services as defined in this Agreement and attached Exhibits. Please refer to Exhibits D-I indicated below for specific scope of work and service terms of each service.

https://cloud.sdsc.edu/v1/AUTH_sdsc-docs/SLA_Exhibits/

SDSC Project Storage: Refer to Exhibit D, "SDSC Project Storage Services"
SDSC Cloud Storage and Compute: Refer to Exhibit E, "SDSC Cloud Storage and Compute Services"
SDSC Backup Services: Refer to Exhibit F, "SDSC Backup Services"
SDSC VM Services: Refer to Exhibit G, "SDSC VM Services"
SDSC Systems Management Services: Refer to Exhibit H, "SDSC Systems Management Services"
SDSC Hourly Labor Services: Refer to Exhibit I, "SDSC Hourly Labor Services"

3. Definitions

3.1 Definitions

3.1.1 ***"Condo"*** storage refers to an arrangement wherein Customer provides funds to purchase a designated amount of storage space which is incorporated into Service Provider managed systems and operated for Customer by Service Provider for a maintenance fee.

3.1.2 "***Customer***" means the party contracting with Service Provider for services provided by Service Provider under this Agreement.

3.1.3 "***Data***" means all information, whether in oral or written (including electronic) form, created by or in any way originating with End Users, and all information that is the output of any computer processing, or other electronic manipulation, of any information that was created by or in any way originating with End Users, in the course of using and configuring the services provided under this Agreement.

3.1.4 "***End User***" means the individual(s) authorized by Customer to access and use services provided by Service Provider under this Agreement.

3.1.5 ***"HIPAA"*** refers to the Health Insurance Portability and Accountability Act of 1996.

3.1.6 ***"RDS"*** refers to the San Diego Supercomputer Center Research Data Services group.

3.1.7 ***"On Demand"*** storage refers either to the arrangement wherein Customer pays a monthly fee for an ad hoc amount of storage capacity within SDSC Cloud Storage and is billed based on actual usage or wherein Customer pays a monthly fee for an allocated storage share in SDSC Project Storage, where the storage capacity allocated to Customer may be modified by Customer request.

3.1.8 ***"PHI"*** and ***"PII"*** refer to "Personal Health Information" and "Personally Identifiable Information," respectively.

4. Costs and Storage Allocations

4.1 COST

See total cost estimates attached as Exhibit A. Please refer to the specific service exhibit listed below for applicable additional billing procedures and methodology.

4.1.1 Project Storage Customers: refer to Exhibit D, "SDSC Project Storage Services"

4.1.2 Cloud Storage and Compute Customers: refer to Exhibit E, "SDSC Cloud Storage and Compute Services"

4.1.3 Backup Customers: refer to Exhibit F, "SDSC Backup Services"

4.1.4 Virtualization (VM) Customers: refer to Exhibit G, "SDSC VM Services"

4.1.5 Systems Management Customers: refer to Exhibit H, "SDSC Systems Management Services"

4.1.6 Hourly Labor Services Customers: refer to Exhibit I, "SDSC Hourly Labor Services"

4.1.7 Rate Adjustments: Service Provider reserves the right to review and adjust rates per the UC San Diego recharge policies. Service Provider will give Customer sixty days' notice in advance of adjusting any storage rates.

4.2 Invoicing and Payment

- For SDSC RDS-provided services, Service Provider will submit a monthly recharge billing to the index number(s) provided by Customer.
- Monthly recharge statements are available for review at http://business.sdsc.edu.
- Customers utilizing UC intercampus transfers for billing will be provided an intercampus transfer form and regularly scheduled invoice for payment. The invoice will provide a breakdown of the service costs by type and usage amounts. SDSC RDS-provided services types are represented in Exhibits D-I.
- Customer must email support@sdsc.edu to update billing information for services provided by this Agreement.
- SDSC Cloud and Backup services billable months run from the 20th of the previous month to the 19th of the current month each month.
- Usage information for all other services is submitted for billing on the 15th of each month.

4.3 Failure to Pay Service Fees When Due

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

- If Service Provider is unable to collect payment when due, Customer's service account will enter unpaid status. Service Provider will attempt to contact Customer using the listed Customer contact email addresses.

- Refer to Exhibits D-I for subsequent non-payment actions as the actions may vary by service type.

4.4 Early Termination of RDS Services

- Customer may opt for early termination of any or all of the services listed in Section 2, Scope of Work, by providing written notice to Service Provider contacts listed in Section 11 of this Agreement thirty days in advance of desired termination date. Service will continue through the last day of the month in which the termination falls, at which time Service Provider will be released from responsibility of providing or maintaining the specified service(s). Customer will have until the termination date to retrieve any data from the terminated service.
- After the termination date, all data, system images, stored backup sets, or other service specific data will be deleted from the service(s) specified in the termination request. Any allocated resources formerly allocated to Customer will be released to Service Provider for reuse at discretion.
- **Customer agrees upon signing this Agreement to release Service Provider of all liability for data after termination date.**

5. Service Provider Responsibilities

5.1 Service-specific Responsibilities

Service Provider shall deliver scope of services for each service as defined by Exhibits referenced in Section 2.

5.2 Technical Support and Notifications

5.2.1 Unscheduled RDS Systems Downtime Communication

- Where applicable, real-time monitoring is provided by Service Provider monitoring systems. Detected downtime of applicable components will generate an immediate email to Service Provider personnel.
- Upon receiving an alert, administrators will make commercially feasible efforts to diagnose and resolve the issue.
- In the case of unscheduled downtime across multiple Customer systems, Service Provider will post incident information during and after incident at http://status.sdsc.edu.
- In the case of unscheduled downtime in localized Customer system(s), Service Provider will provide incident information and analysis to Customer via provided email addresses listed in Exhibit A of this Agreement or to updated email addresses provided by Customer by emailing support@sdsc.edu.
    - During regular business hours, Service Provider staff will make reasonable effort to send incident information within 2 hours. SDSC RDS "Regular Business Hours" are **Monday through Friday from 8:00 AM to 5:00 PM Pacific Time**. For outages lasting longer than 6 hours, further updates will be provided as they become available.
    - If incident occurs outside regular business hours, Service Provider staff will make reasonable efforts to send incident information within 6 hours.
- Within one business day after incident resolution, when applicable Service Provider will provide a high-level written post-incident summary to Direct Customers. Summary will include:
    - Incident cause analysis
    - Incident solution description
    - Recommended preventive measures for future incident mitigation

5.2.2 Planned RDS Maintenance Downtime Communication

- Service Provider will make reasonable efforts to notify Customer at least two weeks prior to planned system outages.
- Reasonable efforts will be made to perform planned system outages outside regular business hours as defined above in Section 5.1.

5.2.3 RDS Systems Technical Support Procedures

- Low and Medium Priority Issues

- Examples: slowness, bug or permissions issues
- Customer will submit support requests via email to support@sdsc.edu. The email will open a support ticket in the Service Provider support system.
- Customer will receive automated receipt email with ticket number acknowledged within 1 hour. Replies to automated receipt email will consolidate support communication within Service provider support system.
- Service Provider will make first response to ticket by close of first following business day. Business hours are defined in Section 5.1.

- High and Critical Priority Issues
  - Examples: outage, inaccessible data
  - Customers can submit a support ticket to support@sdsc.edu or call SDSC Operations: (858) 534-5090. Operations staff are available twenty-four hours per day, seven days a week.
  - SDSC Operations staff will take pertinent information (including incident details and response phone number), and telephone on-call member of SDSC technical team supporting the project.
  - SDSC RDS team will follow-up with Customer and respond to the issue as soon as possible after receiving notification.

5.2.4 Accessibility

Service Provider will provide support as defined in Section 5 directly to Customer. Service Provider is responsible for the security of the hardware operating system platforms, storage media and RDS-maintained software. Customer is responsible for the security features of its own applications and data outside of Service Provider systems. Parties together will determine effective methods to accommodate Customer's business needs while conforming to UC, UC San Diego, UCOP, SDSC, and security policies and procedures.

5.3 Service Provider Points of Contact Updates

Service Provider shall notify Customer of any changes to Service Provider points of contact defined in Section 11 by emailing Customer email addresses provided in Exhibit A.

5.4 Security

Parties shall monitor Service Provider systems to identify security issues. Service Provider reserves the right to immediately quarantine Customer systems or perform other mitigating actions when a security issue is identified.

Service Provider is not responsible for patching software on Customer services unless specifically contracted to do so as defined in Exhibit A. Refer to Section 6.4.4 for Customer software patching responsibilities.

6. User Responsibilities

Users of Service Provider resources shall ensure that the following conditions are met:

6.1 Customer Points of Contact Updates

Notify Service Provider immediately of any changes to the Customer primary technical or business points of contact by sending email to support@sdsc.edu.

6.2 Appropriate Data

Customer and End Users shall ensure that all data stored in Service Provider systems is consistent with all policies noted in this Agreement. Customer should be prepared to demonstrate that all data stored in Service Provider systems is directly related to the project authorized by this Agreement as detailed in Exhibit A. Customers are responsible for ensuring compliance with UC San Diego Minimum Network Connection Standards and all UCOP policies pertaining to IS Security unless the Customer has opted to purchase logical security and systems administration services from Service Provider.

DS RA

6.3 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.

6.4 Data Security

6.4.1 Authentication

Customers and End Users are responsible for the security of their data, for the protection of their passwords, and for ensuring that all necessary security requirements are maintained.

Passwords must <u>never</u> be shared. If Customer believes any password, account, or system has been compromised, Customer should ensure passwords are changed immediately and notify Service Provider of the compromise within one business day.

6.4.2 Regulated Data

No hosted storage services referenced in this document may be used to store regulated data (PII/PHI, etc.). See specific PHI/PII data definitions in Section 6.6 below.

For systems managed by Service Provider under this Agreement, Service Provider agrees to follow industry standard security practices including but not limited to regular patching of operating systems and software maintained by Service Provider, 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 Service Provider systems. Such additional requirements must be documented by Customer and incorporated into this Agreement via signed amendment prior to data storage.

6.4.3 Security Agents

Customer agrees that Service Provider reserves the right to install security agents on Customer systems.

- Agents are used to perform vulnerability scans on a regular basis.
- The results of the scans can be shared with the Customer points of contact for each scanned system.
- When findings are classified, per Industry rating, as either "Critical" or "High", Customer is expected to remediate the findings within ten calendar days of being notified.
- Depending on the severity of the issue and resolution response, the Customer's corresponding campus CISO may also need to be notified.

6.4.4 Software Patching

Customers and End Users are responsible for keeping software installed on Service Provider systems secure and updated unless Service Provider is contracted to perform updates per scope of services defined in Exhibit A.

If Customer-maintained software is identified as compromised, Service Provider reserves the right to immediately quarantine affected systems or perform other mitigating actions and to assess Customer with costs based on SDSC RDS hourly labor rates to cover any and all applicable mitigation efforts.

6.5 Storing Sensitive Information on SDSC RDS Systems

Service Provider services are not intended for unencrypted or encrypted storage of any sensitive information including but not limited to PHI/PII data. Use of these services to store regulated or protected data is strictly prohibited.

6.6 PII and PHI Data

Customer agrees that no Personally Identifiable Information ("PII") as defined by California privacy laws (including California Civil Code sections 56-56.37) or Protected Health Information ("PHI") as defined by the Health Insurance Portability & Accountability Act of 1996 ("HIPAA", 45CFR Parts 160 and 164) shall be transmitted to SDSC under this Agreement. ***Transmission of either PHI or PII by Customer to Service Provider shall be grounds for immediate termination of this Agreement.*** Comingling of data that is PHI or PII with data that is not PHI or PII is prohibited under this Agreement. If Customer finds it necessary to begin transmission of PHI or PII, Customer agrees to contact Service Provider before transmission, in order to enter into a new Agreement for services that cover the appropriate security measures as required by State and Federal laws including HIPAA/HITECH.

6.7 Privacy

Service Provider 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, Service Provider will not use such data for Service Provider 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.

6.8 Backups of Critical Customer Data

Customers and End Users are responsible for keeping a backup of their data outside of Service Provider systems. File systems and archival storage systems are generally reliable; however, data can be lost or damaged due to media failures, hardware failures, user actions, system administrator actions pursuant to client instructions or errors, network failure, power failure, and acts of nature including but not limited to earthquakes, fires, floods, or other Natural disasters.

Note that Service Provider cannot be held responsible for errors or problems with data before its residence in Service Provider systems. The process of transferring data and validating it upon arrival at Service Provider is separate from actual storage of the data. Potential problems include but are not limited to bad hard drives, 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 Service Provider systems to verify that stored and retrieved files are intact. Customer can check files against the MD5 checksums held in the system.

6.9 System Restorations of RDS Managed Systems

In the event of a hardware failure, security incident, failed patch installation, or other issue that requires a customer's physical or virtual system to be reinstalled, SDSC will provide a cleanly installed and patched operating system or perform a full restoration from the most recent valid full backup if customer has an active Service Provider backup service for the system.

- Customer is responsible for reinstallation and configuration of any additional software beyond the base operating system.
- Customer may elect to pay SDSC RDS hourly labor rates to assist with the reinstallation and configuration of software.
- Customer is responsible for storing software installation media and license information, and must provide this for Customer-owned software that is to be installed on the system.

- Software or media provided by Customer will be returned to Customer after successful installation and will not be stored at Service Provider.
- Reinstallation of colocated systems OS or software is not provided unless additional systems management or hourly labor services are requested.

6.10 Policies and Procedures Adherence

Parties agree to follow all applicable Federal, State, University, and SDSC policies and procedures.

7. Entire Agreement.

This SLA sets forth the entire Agreement of the parties with respect to the subject matter herein and supersedes any prior Agreements, oral and written, and all other communications between the parties with respect to such subject matter.

8. Modification of Agreement

Modification of this Agreement shall be discussed and mutually agreed upon in writing by Parties. Notification of potential changes will be made to the Customer more than two (2) weeks prior to any Agreement change taking effect.

9. **Non-Exclusivity**

The Parties acknowledge and agree that each Party reserves the right to supply or obtain any services or products to or from any other client or source during and after the term of this Agreement.

10. **Limitation of Liability**

EXCEPT WITH REGARD TO ITS INDEMNIFICATION OBLIGATIONS, NEITHER PARTY WILL BE LIABLE TO THE OTHER PARTY FOR ANY INDIRECT, SPECIAL, INCIDENTAL, EXEMPLARY OR CONSEQUENTIAL DAMAGES, OR COSTS, INCLUDING, BUT NOT LIMITED TO, ANY LOST PROFITS OR REVENUES, EVEN IF SUCH PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES AND REGARDLESS OF THE LEGAL THEORY UNDER WHICH DAMAGES ARE SOUGHT. **SERVICE PROVIDER DISCLAIMS ALL WARRANTIES EXPRESS AND IMPLIED, INCLUDING WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. IN NO EVENT SHALL TOTAL LIABILITY OF SERVICE PROVIDER UNDER THIS AGREEMENT EXCEED THE AMOUNT PAID BY CUSTOMER FOR THE SERVICES.**

11. Contacts

SDSC Mailing Address
University of California, San Diego
San Diego Supercomputer Center
9500 Gilman Drive MC 0505
La Jolla, California 92093-0505

SDSC Shipping Address
University of California, San Diego
San Diego Supercomputer Center
10100 Hopkins Drive
La Jolla, California 92093-0505

SDSC
SAN DIEGO SUPERCOMPUTER CENTER

SDSC RDS Exhibit A
Scope of Services

Service	Year 1
SDSC Universal Scale Storage - 200 TB minimum allocation @ $70/TB/year. - Email support@sdsc.edu for allocation increases or technical support. - Limited snapshots available for recent accidental file deletion recovery. - Mountable on most campus systems: Linux via NFS and Windows/Mac via SMB. - 100 TB minimum increment. - Payment to be made via Intercampus Recharge to qualify for UC pricing. - USS can also be accessed via an S3-like appliance.	$ 14,000
SDSC Cloud Storage Retention - 4 months of retention of merritt SDSC Cloud Storage (Swift) project @ $1,500/mo. - After retention period ends, SDSC may remove objects from merritt project at will. - If space allows, CDL may request a retention period extension from SDSC	$ 6,000
GRAND TOTAL	**$ 20,000**

DS
RA