Colocation Service Terms

Last Updated: March 24, 2017

The following Service Terms apply only to the specific Services to which the Service Terms relate. In the event of a conflict between the terms of these Service Terms and the terms of the UCSD-Customer Service Agreement or any other agreement with UCSD governing your use of Colocation Services (the "Agreement"), the terms and conditions of these Service Terms apply, but only to the extent of such conflict.

1. Universal Service Terms (Applicable to All Services)

1.1 Customer is required to notify SDSC of any changes to the primary technical or business customer through email sent to support@sdsc.edu.

1.2 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 Customer's Service Agreement. Customers are responsible for ensuring compliance with UCSD 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 SDSC.

1.3 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 Customer's Service Agreement.*** It is illegal to distribute data or software without the approval of the owner, and such distribution is therefore considered a violation of Customer's Service Agreement. Violations may result in immediate termination of services.

1.4 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 the SDSC Cloud 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 the SDSC Cloud. Such additional requirements must be documented by Customer and incorporated into all Customer Service Agreement(s) via signed amendment prior to data storage.

1.5 Privacy. SDSC will use Customer/End User Data only for the purpose of fulfilling its duties under Customer's Service Agreement(s) 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.

1.6 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 SDSC 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 SDSC 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. *Customers that have already entered into Service Agreement(s) for colocation services that cover appropriate security measures are exempt from this section.*

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

2. Technical Support and Notifications

2.1 Communication Regarding Planned Maintenance

- SDSC will make reasonable efforts to notify clients two weeks prior to any planned system outage.
- Reasonable efforts will be made to perform planned system outages outside of regular business hours. Although Customers

often work after hours and on weekends, “Regular Business Hours” is defined as Monday through Friday from 08:00 AM to17:00 PM, PST

2.2 Support and Notification

- For support requests: Please reply to your Footprints Master Ticket email. Please do not open a new support request. If you are unable to locate your master ticket email please contact the SDSC Operations team by emailing operator@sdsc.edu.
- Notification regarding Colocation Services will be provided to the address that is subscribed to the ColoNotice@sdsc.edu mailing list.
- SDSC’s service response goal for notification of outages affecting the SDSC Data Center and Colocation facilities is 60 minutes. All efforts will be made by SDSC and its partners to return equipment or facility to normal service as quickly as possible. Notification will be sent as appropriate.
- SDSC will replace/repair colo hardware based on service agreements and schedules with appropriate vendor(s).

3. Security Compliance

3.1 Physical Access

- No unauthorized access to the SDSC Data Center is permitted. Only individuals sponsored by an SDSC Customer or SDSC Staff member are given access to the SDSC Data Center. The SDSC Data Center is monitored 24x7 by operators to ensure against unauthorized access and adverse environmental impacts (e.g., fire, loss of cooling or power), and that appropriate response is taken. This monitoring ensures that no physical modification, destruction, loss, or theft can occur.
- Multiple building security cameras and the SDSC Data Center’s door access-control system record individual access. Security cameras (CCTV) with DVR recording devices, in lieu of physical intrusion alarms, are placed at the door to the SDSC Data Center, at cage entrances, and the end of each row of racks showing the front and back of each. The operators monitor these systems continuously and respond appropriately (e.g., contact campus police) in the event of an intrusion.
- SDSC Management approves authorized access to both the Data Center itself and to individual cages and issues authorization credentials. The Operations staff maintains the SDSC Data Center and cage access system lists. This lists and the need for access are reviewed every six months.
- Authorized staff gain access to both the SDSC Data Center and cages through separate biometric authentication systems.

These systems verify the identity of a person based on physiological or behavioral characteristics, specifically the vascular pattern on the back of the hand in addition to a PIN that the person provides. When individuals are transferred or terminated, the biometric system is updated accordingly.

3.2 Supporting Systems and Environmental Hazards

- SDSC operators monitor all sources of power in the SDSC Data Center: power generators, HVAC systems, cabling, and the wiring closet. SDSC has a master emergency cut-off switch, located in the Data Center near the cage that is marked and protected by a cover to prevent inadvertent activation. (The East Wing has a circular ring to prevent pulling.) Operations staff is trained in the location and use of this switch.
- Temperature and humidity control systems are located within the HVAC systems. SDSC personnel maintain temperature and humidity levels where the information system resides consistent with American Society of Heating, Refrigerating and Air-conditioning Engineers (ASHRAE) document titled Thermal Guidelines for Data Processing Environments. The temperature and humidity level are monitored continuously by the Operations staff.
- All SDSC equipment in the cage is protected with backup emergency power provided by 3 MW of Uninterruptible Power Supply (UPS) and a 2-MW diesel generator. These systems have power filtering to enable an orderly shutdown. Procedures to support the shutdown are documented in the project's Operations and Maintenance Manual and implemented by authorized system administrators.
- The SDSC Data Center has numerous fire protection mechanisms in compliance with local fire ordinances and requirements of the UC San Diego fire marshal. Fire protection equipment includes separate gaseous and dry-pipe water systems, and a fire extinguisher inside the cage. Fire suppression system shutoff controls are located within the SDSC Data Center, and the Operations staff is trained in their use. In the event of an alarm, Operations personnel and emergency responders are both notified immediately.
- SDSC's Data Center has emergency lighting in compliance with campus safety requirements. SDSC Operations staff maintains a diagram showing emergency lighting and egress.

3.3 Staff and Visitor Access

- Only visitors who are escorted by SDSC staff are allowed in the SDSC Data Center. SDSC's 24x7 operators monitor all visitors to the SDSC Data Center. All visitors must sign in at the door to

the Data Center, with date, name, and purpose. This allows escorted vendors to perform maintenance with systems in place.

- No unescorted visitors are allowed in the SDSC Data Center. Logs are maintained there to track all entry. Additionally, a surveillance camera monitors and records access to the SDSC Data Center and to each cage.

3.4 Checkout Procedures

3.4.1 Internal: Upon departure of SDSC staff (posted last day), building and data center access will be expired. Based on a review of that employees areas of responsibilities, accounts will be deleted and shared passwords will be changed as appropriate.

3.4.2 External: Responsibility falls upon the customer to notify SDSC of personnel changes regarding data center access per SDSC/Customer SLA requirements. SDSC operations staff will audit the access systems annually in conjunction with SLA the refresh to verify all customers departmental staff has not changed.

3.5 Rack Security

3.5.1 East Data Center: Operations will tour the facility during each shift to identify and secure racks that have been left open or unlocked by the customer. Operations will also monitor the rack security system for alarms of this nature. This is part of the service that comes from paying the “compliance security” fee for the electronic locking handles.

3.5.2 West Data Center: Locking kits are available for additional rack security within this facility, but customers are responsible for ensuring their cabinets are properly closed and locked. Operations will close racks that are left unsecure as a courtesy during facility tours or normal business operation, but this is only a courtesy and not a service offering.

3.6 Video retention

Security video footage captured from the SDSC Data Center will be retained onsite for a period on 90 days, and will be accessible to customers via request to SDSC operations and pursuant to applicable UC access and privacy policies and state and local laws. Camera feeds are NOT internet or network accessible.

3.7 Authenticated Data Center Access

Entry points to the SDSC Data Center shall use authenticated access systems to protect against access by unauthorized personnel. The access systems shall record the name of the person accessing the Data Center along with the date and time.

3.8 Access logs and log retention

All access logs to SDSC data center and customer racks will be retained for 180 days, and will be available to customers for their own racks via request to SDSC operations.

3.9 Chain of Custody for Media

SDSC provides remote hands service including hard drive replacement. SDSC will retain these drives for a period of 90 days while the customer schedules removal/destruction. SDSC does not offer or verify on-site media destruction services.

3.10 Escalation Process

All service requests should be handled via the SDSC ticketing system. If no response/acknowledgement is received within 90 minutes, or if this request is critical based on customer impact, please call SDSC Operations at (858)534-5090. This is the 24x7 phone number for SDSC's Operations Center. When calling this number you will need to know your ticket number and your passcode (set with SDSC during the SLA process). Any further needed escalation should be directed to the Data Center Manager, Jeff Filliez jfilliez@sdsc.edu (858)534-8368.

3.11 Deliveries to the Data Center

SDSC requires all deliveries to be received and signed for by authorized individuals.

All shipments sent to SDSC should be addressed as follows:
San Diego Supercomputer Center
ATTN: (your name/department)
10100 Hopkins Dr.
La Jolla, CA 92037

All major shipping companies deliver to our location, and weekend shipments are acceptable. If your shipping requires a phone number please use the Operations number (858)534-5090. Outbound shipping requires the customer to provide a pre-paid shipping label and to schedule any pickups based on their own need.

3.12 Surplus/Salvage Procedure

- SDSC will act as POC and pickup point for UCSD Surplus Sales, but the home department must complete all paperwork.
- For customers outside of UCSD, and surplus/salvage of equipment must be either shipped back to the home site, or have ownership/title of the asset transferred to SDSC.

Procedure for this can be accessed via the Data Center Manager.