

SAN DIEGO SUPERCOMPUTER CENTER**HPC USER RESPONSIBILITIES**

Each SDSC user assumes certain responsibilities when using the resources at SDSC.

1. Only work authorized in the original request for an account is permitted. Programs and data of a personal nature are not authorized. Users should be prepared to justify that all programs and data are directly related to authorized projects.
2. It is illegal to copy and/or distribute proprietary software without the approval of the software owner. Permission must be obtained from the owner of the software before any proprietary software is copied and/or installed on SDSC resources.
3. It is required that users with allocations approved by NSF peer review acknowledge NSF and SDSC support in all publications and send a copy of each to SDSC. Send publications or links to publications to the following e-mail address: allocations@sdsc.edu.
4. Each user is required to protect his or her password(s) and passwords must never be shared. Users who believe a password has been compromised should change that password immediately and notify SDSC security at: security@sdsc.edu.
5. Users are solely responsible for the security of their programs and data. Users are responsible for backing up critical data. Filesystems and archival storage systems are very reliable, however, data can be lost or damaged due to media failures, software bugs, hardware failures, and other problems.
6. Individuals using SDSC resources without authorization, or in excess of their authority, are subject to having all of their activities on the system monitored and recorded by system personnel. In the course of monitoring unauthorized individuals using these resources, the activities of authorized users may also be monitored. By using SDSC resources you consent to such monitoring and are advised that if such monitoring reveals possible evidence of criminal activity, system personnel may provide the evidence of such monitoring to law enforcement officials. Policies in this regard can be found at <http://www.ucop.edu/ucophome/policies/ec/> section IV.B. and <http://security.sdsc.edu/policy/MonitoringPolicy.html>.
7. Violations of SDSC policy can result in removal of access to SDSC resources and possibly civil and criminal prosecution. SDSC Information Technology policies, standard and guidelines are available at <http://security.sdsc.edu/PSG>. You are responsible for reading and following SDSC policies.

I have read the preceding and all SDSC policy documents and understand my responsibilities as an SDSC user.

Name _____ Institution or Company _____
 (Please print)
 Login Name(s) _____ E-mail _____
 (At SDSC site)
 Phone _____ Fax _____ Academic Status _____
 Signature _____ Date _____

To prevent interruption of service, please read, sign, and return this form as soon as possible to:

Rachel Chrisman FAX :858-534-5152
 UC San Diego
 SDSC, MC 0505
 9500 Gilman Drive
 La Jolla, CA 92093-0505