TSCC Acceptable Use Policy

In using the Triton Shared Computing Cluster and associated resources, you agree to comply with the following conditions of use:

1. You will only use TSCC and associated resources to perform work and transmit/ store data consistent with bona fide scientific research (UC users) or the statement of work in your service agreement or research contract (external users).
2. You will respect intellectual property and copyright laws and observe confidentiality agreements, as applicable.
3. You will not use TSCC for financial gain (except in conjunction with legitimate business purposes as specified in the statement of work in your service agreement or research contract) or any unlawful purpose, nor attempt to breach or circumvent any TSCC administrative or security controls. You will comply with all applicable federal, state, and local laws; working with your organization and UCSD to determine what constraints may be placed on you by any relevant regulations such as Export Administration Regulations or HIPAA. *Note: The baseline configuration of the TSCC system is NOT designed to host regulated (e.g. HIPAA, Controlled Unclassified (CUI), etc.) data. If you intend to host regulated data on this system, please contact tscc-support@ucsd.edu.*
4. You will protect your access credentials (e.g., username, private keys, tokens & passwords) that are issued for your sole use. This includes:
   I. Only entering your TSCC password to log in to TSCC resources.
   II. Not sharing any of your TSCC credentials with any other person.
   III. Using a unique password for your TSCC account (UCSD AD password is acceptable for UCSD users).
5. You will immediately report any known or suspected security breach or misuse of TSCC access credentials by emailing tscc-support@ucsd.edu or calling SDSC Operations at (858) 534-5090.
6. UCSD is entitled to regulate, suspend or terminate your access, and you will immediately comply with their instructions.
7. Principal Investigators and external organization points of contact are responsible for properly vetting users on their allocations and by doing so they are attesting that the TSCC username belongs to the intended person. PI's and organizational points of contact will also ensure that users who have access to TSCC via the PI's or organization's allocation follow this AUP.
8. You will have only one TSCC account and will keep your profile information up-to-date.
9. Use of resources and services through TSCC is at your own risk. There are no guarantees that resources and services will be available, that they will suit

every purpose, or that data will never be lost or corrupted. Users are responsible for backing up critical data, or using replicated or backup storage services provided through UCSD.

10. Logged information, including information provided by you for registration purposes, is used for administrative, operational, accounting, monitoring and security purposes. This information may be disclosed, via secured mechanisms, only for the same purposes.
11. Violations of this TSCC policies and/or service provider policies from SDSC and UCSD can result in loss of access to resources. Activities in violation of any laws may be reported to the proper authorities for investigation and prosecution.
12. Please consider acknowledging UCSD's Research Computing program in your publications, presentations, and other media.

Last updated: February 28, 2020