Limited Privileged Access Form
San Diego Supercomputer Center
Privileged User/Local Administrator/limited sudo

Name: ________________________________ **Username:** ___________________ **Date:** ________________

Phone Number: _________________________ **Email:** ____

Reason(s) and purpose I am requesting privileges are as follows:

NOTE: You should discuss privilege requirements with Security Technologies staff FIRST before filling out this form.

System(s) I am requesting privileges on:

Privileges I am requesting (mark an X next to the appropriate entry):

□ Local Administrator privileges on **my own** Windows workstation.

□ Operator privileges (use of operator account, operator sudo privileges, and other operator privileges as necessary

□ User Services privileges (use of sudo on SDSC systems for user support role.)

□ Limited sudo (specific commands) on one or more systems listed above.
This limited sudo and command set will be audited once a year or more by Security Technologies

□ Sudo all on one or more systems listed above.

□ Other: **Specify above in the Reason box**

Privileged access is a serious responsibility. Without understanding the security issues involved in managing a system in a networked environment, you may accidentally or deliberately open security holes, destroy data, invade privacy, or worse. This agreement exists to make you aware of these issues, and to confirm your willingness to use your privileges carefully, ethically, and with the best interests of SDSC and UCSD in mind.

Access does not imply authorization. Having administrative access to a machine does not mean that you may take any action your privileges will permit. Without explicit permission on this form, you may not:

- Add, modify, or remove **user accounts** on any system. Any new or modified accounts will be automatically removed unless prior arrangements have been made with IT Systems.
- Install or enable network services such as windows file shares, web, ftp, or database servers which are visible from systems other than your own unless your machine is relocated to a network designed for such work.
- Use your privileges to view, copy, delete or change files, ownership, or permissions on files that belong to people other than yourself unless you are doing so as part of you job – usually as staff in User Services.
- Use any account other than your own without explicit description on this form.
- Use your privileged access over any unencrypted network connection.
- Use your privileged access to monitor or intercept network communications other than your own.
- Attempt to bypass privilege restrictions, logging systems or install software that allows bypass of privilege limits.
- Install “remote access” software such as PCAnywhere or WinVNC server.
- Perform hardware or OS upgrades without the explicit permission of the appropriate group.
- Leave a machine shut down or disconnected for more than a few minutes (except in case of emergency).
- Remove, alter or disable antivirus software on any system.
- Operate "user offered network services" such as web servers, database servers, etc.
- Install emulation software such as "VirtualPC" or similiar programs.

Any real or perceived violation of these rules or “good practice” can result in disciplinary action. The Manager of Security Technologies is responsible for investigating and adjudicating violations. **You are responsible for contacting Security Technologies staff for removal of privileges upon move to new project or group, or separation/resignation from SDSC.**

Signatures: **(PRINT AND SIGN!)** When signatures are completed, hand form in to the
IT Support Manager (Matthew Kullberg, SDSC room 107) or the Security Manager (Abe Singer, SDSC room 121)

Requestor (you): *(Sign AND print name)*	**Supervisor or project manager signature:** *(Sign AND print name)*

IT Support Manager or Security Manager: (Sign/Print/Date)

Approved: □ **Denied** □ **(Reason)**______________________

You are responsible for abiding by UCSD and SDSC policies available at http://security.sdsc.edu/policy