# Unlimited Privilege Access Form
# San Diego Supercomputer Center
# Unlimited Systems Staff (and others) Access


**Name:** _____ **Username:** _____ **Date:** _____

**Phone Number:** _____ **Email:** _____

Please check the level(s) of access you are requesting and verify that the appropriate signatures appear at the bottom of the form:

☐ **Core Systems Support Staff – Unix or Windows**
(User has Unix root password, sudo "ALL=ALL", Windows adminstrator password, AD administrator rights, etc.)

☐ **Privileged access to core infrastructure systems for a specific purpose**
(DNS changes, file ownership on NFS servers, etc.)

☐ **Extend Access Privileges**
(User has authority to grant privileged access to other users. Give the root password and/or give sudo access)

☐ **Other Privileges**
(Describe below)

**Reasons and purpose I am requesting privileges are as follows (BE SPECIFIC):**

**Privileged access authorization is a serious responsibility. Without understanding the many issues surrounding this access, 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 ethically, carefully, and with the best interests of SDSC and the University in mind.**

**By signing this document you are certifying that you have read, understand, and agree to the items on this page and the second page. UCSD and SDSC policies are your responsibility and are available at http://security.sdsc.edu/policy.**

***RIGHTHAND SIDE SIGNATURES ON THIS FORM CANNOT COME FROM ANYONE OTHER THAN AN SDSC MANAGER OR DIRECTOR!***

| **Requestor (you):** *(Sign AND print name)* | **IT or Production Systems Manager or Director signature:** *(Please Sign AND print name)* ***AND Security Technologies Manager signature*** *(Sign and print)* |
|---|---|

# *READ THE SECOND PAGE!*

# Unlimited Privilege Access Form
# San Diego Supercomputer Center
# Unlimited Systems Staff (and others) Access

**Access does not imply authorization**. Having administrative access to a machine does not mean that you amy take any action your privileges will permit. For example, if you have root on a server to examine system logs or assist in installing software, this does not grant authorization to change the configuration of the machine, to reboot the machine (even via the power switch, except in emergencies) or to add or remove user accounts, etc.

**Things you're agreeing to:**

**I have read and will abide by UCSD and SDSC policies available at http://security.sdsc.edu/policy.**

I understand that I am accountable for everything done via my account. I will make every effort to prevent others from using my account or privileges. I will immediately notify Security Technologies staff if I believe my account has been comprmised.

**Passwords:** Because anyone who knows my password can gain root access, **only I will know my password**. I will keep it secure, and will never leave it in an unencrypted file, including but not limited to auto-login files and scripts. **My password will be difficult to guess, and will follow good password guidelines**. Should I suspect that anyone other than myself knows my password, I will change it immediately *and* notify Security Technologies. If an administrative group discovers that my password can be guessed or has otherwise been compromised, my accounts may be disabled without warning until my password is changed.

**Network security**: I will always ensure that ALL network connections over which I type my password (including all intervening login sessions) **are encrypted**, since even on a well-managed network it is possible for a compromised machine to run unnoticed. I will assume that passwords I type could be sniffed if they go unencrypted over the network. This includes remote xterms unless they are traveling over a 100% encrypted connection. **If I do not understand what this means, I will not sign this form!**

**Logging:** I understand that sudo commands and other uses of my privileges are logged. **I will do my best to use sudo so my actions can be logged instead of using the root password.**

**Crippled hosts:** If I cripple a host, I will notify the appropriate administrative group immediately, providing a detailed description of what happened. I understand that a crippled host may be reinstalled with the standard system image ("reference system").

**Configuration changes:** I will not make changes to any host's operating system or install any privileged software unless my access was granted for the purpose of my doing so. This includes hardware and network configuration, files in system directories, and physical location. If I need something done that falls outside of the range of activities for which my access was granted, I will contact the appropriate administrative group.

**Files you don't own:** I will not use my privileged access to view, copy, delete or modify anyone else's files, directories or email without their explicit permission in advance for each occurrence unless my security duties compel me to do so. This includes the modification of user and group ownership and permissions. Failure to do so is a serious violation of University policy.

**Network monitoring:** I will not use my privileged access to monitor or intercept network communications other than my own without explicit permission. Failure to do so is a serious violation of University and SDSC policy.

**Electronic mail privacy:** The privacy of electronic mail must be maintained in accordance with federal law and UCSD policy. Retrieving a copy of any person's mail (for example, your own) from somebody else's mailbox is expressly prohibited!

**Account changes:** I will not attempt to create or change user's login accounts, passwords, access rights, groups, home directory location, mail host, or any other user information unless I am authorized and trained to do so.

**Changes:** I will **notify Security Technologies if I go on an extended leave of absence, no longer need my privileged access, move to a new SDSC group or resign/separate from SDSC**.

**Providing access to others:** I will not disclose the root password to anyone except in emergency situations. **The root password should only be distributed by Security Technologies staff**. Whenever I disclose the root password for any reason, I will notify Security Technologies and the appropriate administrative group immediately. **I will not extend access privileges to anyone who has not filled out the appropriate form, and I will only do so if my access on this form allows me to extend these privileges.**

**Questions:** If I have ANY questions regarding the use of my privileges or related topics, I will consult with my supervisor and/or Security Technologies staff before proceeding.