

**Privileged Access Usage Agreement**  
**Cooperative Association for Internet Data Analysis**  
**University of California, San Diego**

The purpose of this document is to outline the general expectations of all users given “root” access on any CAIDA machine. **CAIDA senior staff have the authority to disable logins immediately and take additional disciplinary action, including termination of employment, for failure to comply with this agreement.** In general, privileged access to any machine does not give you any additional rights, only responsibilities.

Any account with privileged access by virtue of sudo or special groups is considered a privileged account. All privileged accounts (this means yours since you are signing this) must be protected as follows:

- 1) Privileged access to any system is to be used only for the purpose it was given. Use of privileged access for any unauthorized purpose is prohibited. You shall not execute any commands as a privileged user to gain unwarranted access to private information. In responding to problems, it **IS** appropriate to access as much data as necessary to resolve the problem. It **IS NOT** appropriate to use sudo to read someone’s mail, or to browse someone’s files.
- 2) Your password must be changed at least twice a year, or immediately if guessed by a password cracker or seen by another person (even if only partially). Be sure you never change your password across an unencrypted network connection. You must choose a password that is sufficiently difficult to guess, that is not based on a dictionary word, and that contains mixed case, numbers, and/or punctuation. You must use a different password on non-CAIDA machines (e.g. SDSC, UCSD, or AOL). Many systems do not require the use of secure login mechanisms such as ssh, and consequently passwords may be intercepted during ordinary use. By using different passwords in separate domains, you prevent an intruder from gaining access to CAIDA machines even if they have already compromised other systems.
- 3) You must not give your password to **anyone** under **any** circumstances. Logging in for guest and allowing them to use your account temporarily is acceptable provided it is completely supervised by you, or if you completely trust the borrower.
- 4) Root shells are not appropriate unless absolutely necessary. When a root shell is used, preface each command with ‘sudo’ so the commands are logged.
- 5) Information gained through privileged access is **privileged** and should not be repeated. You are personally responsible for ensuring that any information you may obtain through privileged access is not used by yourself, or anyone else. Just forget you ever saw it.
- 6) This agreement supplements the agreement governing general use of accounts.

I understand and will abide by the above terms and conditions. If the propriety of any situation is unclear, I will ask for clarification from the CAIDA PI rather than making assumptions. I understand that my sudo privileges may be revoked if the terms and conditions are not adhered to.

Login: \_\_\_\_\_ Email: \_\_\_\_\_

Printed Name: \_\_\_\_\_ Phone: \_\_\_\_\_

Signature: \_\_\_\_\_ Date: \_\_\_\_\_