Sudo Access to Workstations

Adopted 15 April 2009; Revised 12 November 2014

Consistent with the Department's mission to educate the next generation of astronomers, we recognize the need to train our students not only in astronomy, but also in the skills which will be important to them as future educators, researchers, and scientists. These skills include developing expertise in information technology. Appropriately, then, faculty, students, and staff in the Department need to have opportunities to maintain and support their desktop computing environments. These opportunities include root or administrator privileges via "sudo" on computers, including unix-based systems.

Users with root privileges must be cognizant of University policies, security requirements, and safe practices, and must conform to such policies. Written acknowledgement of these responsibilities will be required before sudo access is granted. Users should log and report new software installations and significant activities performed under sudo. Users who need help to recover from mistakes made under sudo should expect to be involved in repairing their desktops.

Access is defined at four levels:

- **Basic user access** runs applications, with no sudo access.
- **Command sudo access** permits a limited set of commands which can be specified for individual users.
- **Full sudo access** is provided to all commands except (1) shells (/bin/bash, /bin/tsch, etc), (2) editors (emacs, vi, etc), and (3) programs known to permit shell or system call access (perl, scheme, etc). File editing is still permitted but granted through the use of sudoedit (aka sudo –e).
- **Unrestricted sudo access** allows complete and unrestricted sudo access. Anyone with unrestricted access is strongly discouraged from using sudo to invoke a root shell unless absolutely necessary.

Faculty and staff in the department will be granted Full Access or Unrestricted Access on machines they own or control if desired.

Graduate students in the department will be granted Full Access or Unrestricted Access on their desktop upon request to the department chair or to the owner of the machine, as appropriate.

Undergraduate students and guests will generally be restricted to Basic User Access, except in cases where academic, research, or support work requires a higher level of access. In such cases, a higher level of access must be approved by both the faculty advisor and the department chair.

Access at the full or unrestricted levels to various *departmental* machines may be granted under special circumstances in consultation with the faculty involved, the department chair, and IT senior staff.

In keeping with our educational mission, IT staff will provide training opportunities for faculty, staff, and students to learn the skills needed to maintain and support desktop computing environments.

Note that continued access to sudo privileges presumes that users follow good practices. For example:

- Don’t change the root password on your machine.
- Don’t add user accounts to the system.
- Don’t grant sudo access to any user.
- Don’t run network daemons: i.e., no ircd, no ftpd
- Don’t use sudo to run a shell: e.g., “sudo bash”, or to just become root via “su”.
- Don’t use sudo to “su” to another user.
- When in doubt, ask the system administrators.