Privileged Account Access Policy

1.0 Purpose

The purpose of this document is to set forth NOAO's policy regarding which person(s) will be allowed privileged account access (root, administrator) to NOAO computer systems.

2.0 Scope

This policy applies to all computing infrastructure that is owned by NOAO or is administrated or managed by NOAO's CIS Departments or IT staff in other NOAO departments.

3.0 Policy

- Root and admin-level access is restricted to a *limited* number of people who have a true *need-to-know* requirement for system access, control and modification.

- Privileged Account passwords should be changed quarterly and the need-to-know list should also be reviewed quarterly.

- Users must login to a particular computer system using their own login name and credentials and become privileged through use of the "su" or "sudo" commands, or equivalent for *NIX systems.

- Machine "owners" that control their own desktop or laptop system may be given individual root/admin-level passwords. System staff shall also maintain root/admin-level passwords on these machines.

- When any employee knowing root-level passwords leaves NOAO employment, all root-level passwords must be changed immediately.

- Root passwords shall not be written down on paper or stored electronically. A paper copy stored under lock and key is acceptable (and prudent).

- Root passwords, as far as is practical, should be different on different machines.

4.0 Revision History

First Edition: March 15, 2007
Updated: February 11, 2008