# NOAO Server Security Policy

## 1.0 Purpose

The purpose of this policy is to establish standards for the configuration of server equipment that is owned and/or operated by NOAO.

## 2.0 Scope

.This policy is specifically for equipment on the internal NOAO network, whether available directly from outside the NOAO network via the public Internet or devices specifically configured or firewalled as internal-to-NOAO access only. Desktop machines are not relevant to the scope of this policy.

## 3.0 Policy

### 3.1 Ownership and Responsibilities

All internal servers deployed at NOAO must be owned by an operational group that is responsible for system administration. If the server is operated by a group outside the two CIS departments, information about the server, particularly a point-of-contact, will be provided to the CIS Departments and kept up to date.

### 3.2 General Configuration Guidelines

3.2.1 Operating System configuration should be done in collaboration with CIS.
3.2.2 Services and applications that will not be used must be uninstalled or disabled where practical.
3.2.3 Access to services should be logged and/or protected through access-control methods such as TCP Wrappers, if possible.
3.2.4 The most recent security patches must be installed on the system as soon as practical, the only exception being when the immediate application of patches/updates would interfere with business requirements.
3.2.5 Trust relationships between systems are a security risk, and their use should be avoided. Do not use a trust relationship when some other method of communication will do (i.e., use ssh instead of rsh).
3.2.6 Always use standard security principles of least required access to perform a function, i.e., do not use root when a non-privileged account will do.
3.2.7 If a methodology for secure channel connection is available (i.e., technically feasible), privileged access must be performed over secure channels, (e.g., encrypted network connections using ssh or IPSec).
3.2.8 Servers should be physically located in an access-controlled environment.
3.2.9 Servers are specifically prohibited from operating in uncontrolled cubicle areas.
3.2.10 Servers will be backed up according to the *NOAO Backup Policy.*

### 3.3 Monitoring

3.3.1 All security-related events on critical or sensitive systems must be logged and audit trails saved.
3.3.2 Security-related events will be reported to the CIS Department, who will review logs and report incidents. Corrective measures will be prescribed as needed. Security-related events include, but are not limited to:
3.3.2.1 Port-scan attacks
3.3.2.2 Evidence of unauthorized access to privileged accounts
3.3.2.3 Anomalous occurrences that are not related to specific applications on the host.

### 3.4 Compliance

3.4.1 Audits will be performed on a regular basis by the CIS Departments..
3.4.2 Every effort will be made to prevent audits from causing operational failures or disruptions.

**4.0 Revision History**

First Edition: March 15, 2007
Revised: September 16, 2009