

# NOAO Server Security Policy

## 1.0 Purpose

The purpose of this policy is to establish standards for the base configuration of internal server equipment that is owned and/or operated by NOAO. Effective implementation of this policy will minimize unauthorized access to NOAO proprietary information and technology.

## 2.0 Scope

This policy applies to server equipment owned and/or operated by NOAO.

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 and Lab equipment 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. Approved server configuration guides must be established and maintained by each operational group, based on business needs and approved by the CIS Departments. Operational groups should monitor configuration compliance and implement an exception policy tailored to their environment. Each operational group must establish a process for changing the configuration guides, which includes review and approval by the CIS Departments.

3.1.1 Servers must be registered within the corporate enterprise management system. At a minimum, the following information is required to positively identify the point of contact:

3.1.1.1 Server contact(s) and location, and a backup contact

3.1.1.2 Hardware and Operating System/Version

3.1.1.3 Main functions and applications, if applicable

3.1.2 Information in the corporate enterprise management system must be kept up-to-date.

### 3.2 General Configuration Guidelines

3.2.1 Operating System configuration should be in accordance with approved CIS Departments guidelines.

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.

### **3.3 Monitoring**

3.3.1 All security-related events on critical or sensitive systems must be logged and audit trails saved as follows:

3.3.1.1 All security related logs will be kept online for a minimum of 1 year.

3.3.1.2 Weekly full backups of logs will be retained for at least 1 month.

3.3.1.3 Monthly full backups of logs will be retained for a minimum of 2 years.

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 authorized organizations within NOAO.

3.4.2 The internal audit group of the CIS Departments, in accordance with the NOAO Audit Policy, will manage audits. The CIS Departments will filter findings not related to a specific operational group and then present the findings to the appropriate support staff for remediation or justification.

3.4.3 Every effort will be made to prevent audits from causing operational failures or disruptions.

### **4.0 Revision History**

First Edition: March 15, 2007