

# Audit Policy

## 1.0 Purpose

The purpose of this document is to set forth a policy regarding network security and vulnerability scanning performed by the CIS Departments of NOAO. CIS shall utilize an assortment of packet, port and application scanners, (such as Nessus, Snort, Nmap and Wireshark (formerly known as Ethereal) to perform electronic scans of NOAO's workstations, servers, networks, routers and/or firewalls or any other network-connected system at NOAO.

Audits may be conducted to:

- Ensure integrity, confidentiality and availability of information and resources.
- Investigate possible security incidents to ensure conformance to NOAO security policies.
- Monitor user or system activity where appropriate.

## 2.0 Scope

This policy applies to all equipment and computing infrastructure that is owned or leased by NOAO or is connected to NOAO's network infrastructure regardless of ownership. This policy also covers any computer and communications devices that are present on NOAO premises, but which may not be owned or operated by NOAO. CIS will not perform Denial of Service activities without prior notice.

## 3.0 Policy

The CIS Departments of NOAO are hereby authorized to access NOAO network and computer infrastructure for the purpose of performing network security and vulnerability audits.

This access may include:

- User level and/or system level access to any computing or communications device.
- Access to information (electronic, hardcopy, etc.) that may be produced, transmitted or stored on NOAO equipment or premises. Such access, other than as incidental to normal network and computer maintenance, will require prior approval of the NOAO Director.
- Access to work areas (labs, offices, cubicles, storage areas, etc.).
- Access to interactively monitor and log traffic on NOAO networks.

### 3.1 Outside Networks.

In cases where NOAO does not control the network and/or Internet service is provided via a second or third party (such as the University of Arizona), these parties are required to approve scanning in writing if scanning is to occur outside of the NOAO network. By signing this agreement, all involved parties acknowledge that they authorize CIS to use their service networks as a gateway for the conduct of these tests during the dates and times specified.

### 3.2 Service Degradation and/or Interruption.

Network performance and/or availability may be affected by the network scanning.

## 4.0 Revision History

Updated:	May 16, 2006
Updated:	July 13, 2006
Updated:	July 14, 2006
Updated:	November 19, 2006
Updated:	December 6, 2006
Revised:	April 21, 2009