

NOAO Remote Access Policy

1.0 Purpose

The purpose of this policy is to protect NOAO's electronic information from being inadvertently compromised by authorized personnel using a dial-in, remote ssh connection, remote VPN connection or any network connection.

2.0 Scope

The scope of this policy is to define appropriate remote access and its use by authorized personnel.

3.0 Policy

- Remote access to NOAO computing facilities must be done in a secure manner that does not reveal passwords or data. No Internet protocols that pass login credentials in clear-text will be allowed. Thus telnet, rlogin and the other Berkeley r-commands and non-anonymous FTP must be blocked. Email servers must use protocols that do not transfer clear-text passwords.
- Preferred techniques for remote access feature data encryption as well as secure exchange of login credentials; examples include ssh version 2 and VPN tunnels.
- NOAO employees and authorized third parties (staff, management, visitors, researchers, students, system administrators, vendors, etc.) can use remote connections (dial-in, ssh version 2 or VPN) to gain access to the corporate network. Information and account setup for remote access connections may be obtained through the CIS departments.
- Dial-in access is strictly controlled, using password authentication.
- Remote ssh connections will use, if at all possible, certificate authentication instead of password authentication. Ssh connections to particular machines will be restricted to particular subsets of IP space through the use of firewall rules or, if necessary, /etc/hosts.allow files. Ssh version 1 is insecure; only version 2 of the protocol is acceptable.
- VPN connections are allowed on a case-by-case basis and require the installation of a client on the remote machine.
- It is the responsibility of employee(s) with remote access privileges to ensure non-employees do not use their remote connection to NOAO to gain access to company information system resources. An employee who is granted remote access privileges must remain constantly aware that connections between their location and NOAO are literal extensions of NOAO's corporate network, and that they provide a potential path to the company's most sensitive information. The employee and/or authorized third party individuals must take every reasonable measure to protect NOAO's assets.

Thus the local network supporting the machine conducting the remote access connection to NOAO must be kept "clean" of malware by proper use of anti-virus and firewall technology.

- Note: Dial-in and remote VPN accounts are considered "as needed" accounts. Account activity is monitored, and if a dial-in account is not used for a period of six months the account will expire and no longer function.

4.0 Revision History

First Edition: March 15, 2007

Updated: September 28, 2009