

DRAFT

COMPUTER INFRASTRUCTURE SERVICES

NOAO Cybersecurity and Acceptable Use Policy

1.0 Overview

The mission of the National Optical Astronomy Observatory (NOAO) is to provide the best ground-based astronomical telescopes to the nation's astronomers, to promote public understanding and support of science, and to advance all aspects of US astronomy. Computers and network resources play an important and essential role in fulfilling the mission of NOAO. In keeping with this mission, NOAO endeavors to provide a safe and secure computing environment.

Computing resources (hardware, software, and data) are vital assets. All users of NOAO computing resources need to be aware of and respect the value of these resources. By using these resources all users become members of a community responsible for ensuring that data is kept confidential, reliable, and available, and that the integrity of NOAO computing resources is not jeopardized.

NOAO's intentions for publishing a Cybersecurity and Acceptable Use Policy are not to impose restrictions that are contrary to NOAO's established culture of openness, trust and integrity. Rather, by defining a framework and a set of policies for "safe computing," NOAO is committed to protecting employees, partners and the Observatory itself from legal liability, computing facility downtime and the loss or corruption of irreplaceable data.

Effective security is a team effort involving the participation and support of every NOAO employee, visitor and affiliate who deals with data and/or data systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

NOAO is responsible for the protection, preservation and improvement of the telescopes and instruments at our facilities and for the acquisition, storage and propagation of useful and valid scientific datasets arising from these telescopes and instruments. We must constantly keep in mind as we use or program our computing facilities: are we committing sins of commission or omission that could cause datasets to become corrupted or cause damage to the telescopes and facilities, or even,

endanger staff or visitors? This policy is written to try and eliminate such sins.

2.0 Purpose

The purpose of this policy is to provide a framework for the implementation and enforcement of computer and network security policies at NOAO and to outline the acceptable use of computer equipment at NOAO. These procedures, rules, restrictions and guidelines are in place to protect the employees, visitors and affiliates of NOAO and the Observatory itself. Inappropriate computer use exposes NOAO to risks including malware attacks, compromise the integrity of our data, computers, networks and services and to legal liability.

3.0 Scope

This policy applies to staff, employees, visitors, students, contractors, consultants, temporaries, and other workers at NOAO, including all personnel affiliated with third party "partner" institutions. 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.

4.0 Policy

4.1 Data and Privacy

1. Stand-alone and network attached systems, including but not limited to computer equipment, accounts, data and files on this computer equipment, and the software and operating systems that run on this computer equipment are the property of NOAO. These computing resources are to be used for business purposes in serving the interests of the Observatory, and of our clients and partners in the course of normal operations. Limited personal use of NOAO computing resources is permitted (see [item 4.2.2](#) below).
2. While NOAO's network administration desires to provide a reasonable level of privacy, users should be aware that the data they create on Observatory systems remain the property of NOAO. Because of the need to protect NOAO's network, NOAO management cannot guarantee the confidentiality of information stored on or passing through any network device belonging to NOAO. Each user must recognize that risks exist with regard to the confidentiality of personal email, data, files and activity logs due to system limitations, software bugs, unauthorized activity, and potential system failures.
3. NOAO management reserves the right to access and disclose all files and all communications sent over its information systems. Such access, other than as incidental to normal network and computer maintenance, will require the prior approval of the NOAO Director. See [NOAO's Network Audit Policy](#).
4. NOAO requires that confidential or sensitive data be encrypted. For guidelines on encrypting email and documents, see [NOAO's Acceptable Encryption Use Policy](#).

5. Data contained in NOAO computing facilities must be backed up. Backup procedures vary with the type of system (laptop versus personal workstation versus server) and the value of the data. See [NOAO's Backup Policy](#).
6. NOAO reserves the rights to limit, restrict, or extend computing privileges and access to its computing resources. Data owners, whether departments, staff, students, or visitors, may allow individuals other than NOAO staff, visitors, and students access to information for which they are responsible, subject to approval from the relevant program administrators.
7. Data services and facilities provided over the Internet to people unaffiliated with NOAO will abide by and prominently highlight on Web sites the [NOAO Internet Privacy and Conditions of Use Policy](#).

4.2 General Use

1. Every authorized user of NOAO computing resources is responsible for the integrity of these resources. All users of computing systems must respect the rights of other computing users, respect the integrity of the physical facilities and controls, and respect all pertinent license and contractual agreements.
2. Users are responsible for exercising good judgment regarding the reasonableness of personal use of Observatory computing resources. Using NOAO computing resources for staff professional development is an appropriate use of resources. Computing resources should not, however, be used to solicit or influence others to become involved in commercial ventures, religious or political causes or outside organizations. If there is any uncertainty, employees should consult their supervisor or manager or Human Resources.
3. NOAO encourages staff members to develop Web home pages to communicate professional activities (contact information, NOAO projects, research interests, publications, CV, meetings and so on). Furthermore, NOAO encourages staff members to share their human side, particularly their enthusiasm for astronomy, through their home pages. Therefore, personal content (family, friends, hobbies, favorite links and so on) may be included on home pages with the understanding that the NOAO Web pages are the public face of our institution and all content should be consistent with this fact. Examples of inappropriate content include material in poor taste, religious or political discussions and promotion of a business.

4.3 Cybersecurity

1. Users of NOAO computing facilities must be aware of any confidential information that they work with. Examples of confidential information include but are not limited to: Personally Identifiable Information (PII), Observatory private and strategic information, confidential medical and HR information and research data protected by proprietary time limits. Confidential information should be stored on server class computers (rather than desktop systems), backed up and encrypted. Employees should take all necessary steps to prevent unauthorized access to this information. Such steps might include access controls and physical security. See NOAO's [Server Security Policy](#) and [Backup Policy](#).

2. Users of NOAO computing facilities must be aware of the importance of the information they work with. Datasets that are indispensable to the operation of NOAO must be protected to a much higher standard than less important datasets. These data must be stored on protected servers, rigorously backed-up and be an integral part of NOAO's business continuity planning. See [NOAO's Server Security Policy](#) and [Backup Policy](#).
3. Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts. System level passwords should be changed at least once every six months; user level passwords should be changed at least once every year. Under no circumstances shall passwords be stored as clear-text on servers. Passwords should be nontrivial, different from those used previously and different for each login domain. See the document [NOAO's Guidelines for Choosing a Good Password](#) for more information.
4. System level and/or "Superuser" passwords will be distributed to users and administrators according to [NOAO's Privileged Account Access Policy](#). All systems must be configured to disallow remote logins as root/superuser/administrator: users must first remotely login to a system as themselves and then authenticate as "root."
5. The NOAO CIS Departments reserve the right to run password cracking programs against the password files on NOAO computer systems to check for trivial and easy-to-guess passwords.
6. To keep personal systems safe from "browsers," all PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 30 minutes or less, or by logging-off or locking the desktop when the machine will be unattended. Physical access controls for server class machines should be implemented according to [NOAO's Server Security Policy](#).
7. If at all possible, confidential information shall not be stored on laptops or portable disk drives (including "thumb drives"). If it is absolutely necessary to carry confidential information on portable devices, the information **must** be encrypted.
8. Because information contained on portable computers is especially vulnerable, special care should be exercised. Protect laptops in accordance with the [Laptop Security Tips](#). Specifically, use a laptop security cable. Make sure that Operating System patches and virus definitions are kept up-to-date on laptops even if they are not connected to the NOAO network.
9. Wireless Access Points must be installed by NOAO's CIS Departments according to [NOAO's Wireless Access Policy](#). "Rogue" Access Points are not allowed. The CIS Departments reserve the right to confine hosts connected via wireless to "untrusted" portions of the NOAO network.
10. Users must take care to wipe all data from computer equipment that is being destroyed, donated or placed on a surplus list. Simply deleting files at the Operating System level is not sufficient. Contact the CIS Departments for wiping services. Make sure that tapes that are leaving service have been wiped of data.
11. All hosts connected to the NOAO network must have a designated administrator. In general, users will not be the administrator of their desktop or laptop computers and will not utilize

administrator privileges. Exceptions will, of course, be made when an employee's job function requires that he or she be the administrator of their computer. However, the CIS Departments reserve the right to require a signed agreement (countersigned by the employee's supervisor) between the employee and CIS specifying that the employee/administrator will apply security patches, will install appropriate security software, will maintain back-ups and will maintain their computer to an appropriate and professional standard.

12. All hosts running the Windows Operating System that are connected to the NOAO Internet/Intranet/Extranet, whether owned by the user, NOAO or a partner organization, shall be continually executing approved, centrally-managed virus-scanning software with a current virus database. Itinerant laptops and virtual PCs running "inside" emulators such as VMware or Virtual PC are explicitly included in this policy. Exceptions must be approved in writing by the employee's manager and network administration. The CIS Departments may specify that computers running older releases of Windows may not be connected to the network.

13. Administrators of all hosts connected to the NOAO network, whether owned by the user, NOAO, or a partner organization must install, as soon as practical, security-related operating system patches.

14. Users must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan-horse code. Similar caution applies to surfing unknown web sites. Think twice before clicking on that URL!

15. The NOAO network shall be protected by firewalls that, by default, block all packets arriving from the "outside." If necessary, specific rules exposing specific ports on specific machines will be installed by the CIS Departments. The CIS Departments reserve the right to block outgoing traffic as well.

16. As far as possible, the log files from NOAO computers (especially web, e-mail and ftp servers) will be collected by specified log servers, subjected to nightly reporting programs whose results are sent to the CIS Departments and kept for a period of at least one year.

17. Remote access to NOAO computing facilities and networks must be done in a secure manner that does not reveal passwords or data, i.e., no protocols that pass login credentials in clear-text. Thus telnet, rlogin, rcp, rexec, rcmd and non-anonymous FTP will be blocked at the firewall. 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/scp version 2 and VPN tunnels. See [NOAO's Remote Access Policy](#).

18. Transactions between computers on the internal network must be authenticated and not presume on trust relationships. In other words, use scp to copy files instead of rcp and make sure your rsync transactions use ssh.

19. Security breaches and incidents will be handled according to the [NOAO Security Incident Response Policy](#).

20. In the case of a security breach or incident, the CIS Departments reserve the right to disconnect any machine(s) from the NOAO network or to cut off access from the NOAO network to the Internet.

21. Users should report unauthorized use of computing resources, apparent violations of this policy or subsidiary policies or observed gaps in system or network security to your project director, supervisor, system administrator, network security administrator or other appropriate NOAO authority immediately upon discovery.

22. The CIS Departments shall conduct periodic cybersecurity awareness training for all staff members.

4.4 Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is an employee of NOAO authorized to engage in any activity that is prohibited by NOAO or AURA policy or is illegal under local, state, federal or international law while connected to and utilizing NOAO-owned computing resources.

The list below is by no means exhaustive, but an attempt to provide a framework for activities which fall into the category of unacceptable use:

1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by NOAO is prohibited.
2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music and video, and the installation of any copyrighted software for which NOAO or the end user does not have an active license is prohibited.
3. Exporting software, technical information, encryption software or technology in violation of federal export control laws is illegal. The appropriate management should be consulted prior to export of any material that is in question.
4. Introduction of malicious programs into the network or any server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.) is prohibited.
5. Revealing your account password to others or allowing use of your account by others is prohibited. This includes family and other household members when work is being done at home.
6. Using a NOAO computing asset to actively engage in procuring or transmitting material that

is in violation of NOAO or AURA policies regarding sexual harassment or hostile workplace or in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction is prohibited.

7. Making fraudulent offers of products, items, or services from any NOAO account is prohibited.

8. Effecting security breaches or disruptions of network communication is prohibited. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, ping floods, packet spoofing, denial of service, etc.

9. Port scanning or security scanning is expressly prohibited unless prior permission is received from NOAO network administration.

10. Executing any form of network monitoring which will intercept data not intended for the employee's host is prohibited, unless this activity is a part of the employee's normal job/duty.

11. Circumventing user authentication or security of any host, network or account is prohibited.

12. Running password cracking programs is prohibited unless prior permission is received from NOAO's CIS Departments.

13. Interfering with or denying service to any other user is prohibited (for example, a denial of service attack).

14. Providing information about, or lists of, NOAO employees to parties outside NOAO is prohibited.

15. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam) is prohibited.

16. Any form of harassment via computer based communication (including but not limited to email, text messaging and web blogging) whether through language, frequency or size of messages is prohibited.

17. Unauthorized use, or forging, of email header information is prohibited.

18. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type is prohibited. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups web forums (newsgroup spam) is prohibited.

19. Downloading or viewing content of a pornographic and sexually offensive nature is prohibited.

5.0 Compliance and Enforcement

1. NOAO reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy and all subsidiary policies. Thus, for security and network maintenance purposes, authorized individuals within NOAO may monitor equipment, systems and network traffic at any time, per [NOAO's Network Audit Policy](#).
2. NOAO will undertake periodic self-audits conducted by the joint CIS staffs to align actual practices with these policies. If necessary and appropriate, audits by external organizations will be arranged.
3. Observed violations of this policy, or any subsidiary policy, will result in an immediate cut-off of network access.
4. Any employee found to have violated this policy, or any subsidiary policy mentioned herein, may be subject to disciplinary action, up to and including termination of employment as well as possible civil and/or criminal prosecution.

6.0 Use of NOAO Computing Facilities by Partner Institutions

Employees and affiliates of NOAO Partner Institutions are implicitly bound by this Acceptable Use Policy when they use NOAO's computing facilities and network infrastructure. Special case exceptions to this policy shall be negotiated between NOAO and Partner Institution Management.

Powers reserved above to the NOAO Director shall be shared by the NOAO Director and the Partner Institution Management where applicable.

Violations of this policy, or any subsidiary policy mentioned herein, by employees or affiliates of Partner Institutions may be reported to Partner Institution Management.

7.0 Revision History

First Edition: March 15, 2007
Revised: April 21, 2009
Revised: September 21, 2009
Revised: March 3, 2010
Revised: March 30, 2010
Revised: May 20, 2010

-
- [NOAO Acceptable Encryption Use Policy](#)
 - [NOAO Network Audit Policy](#)
 - [NOAO Backup Policy](#)
 - [NOAO Laptop Security Tips](#)
 - [NOAO Guidelines for Choosing a Good Password](#)
 - [NOAO Privileged Account Access Policy](#)
 - [NOAO Remote Access Policy](#)

- [NOAO Server Security Policy](#)
- [NOAO Wireless Access Policy](#)
- [NOAO Security Incident Response Policy](#)
- [NOAO Internet Privacy and Conditions of Use Policy](#)

Computer Infrastructure Services, National Optical Astronomy Observatory, 950 N. Cherry Ave., P.O. Box 26732, Tucson, AZ 85726, Phone: 520-318-8100, FAX: 520-318-8360

Last updated: 05/20/2010 19:23:55