Steward Observatory Computer Operating Agreement

January 20, 2004

This is the operating agreement for equipment attached to the Steward Observatory computer network, defined for these purposes to be any network that the Computer Support Group (CSG) maintains, including networks in the Cherry Street buildings, the Mirror Lab, the mountain Observatories, etc.

Each person responsible for a computer connected to the Steward network will be required, yearly, to sign a connection agreement and to provide the information requested on the attached form.

Every device connected to the network must be identified with a responsible person in addition to the owner of the computer. This person can elect to maintain the computer or can elect to have the computer support group provide maintenance. Individuals choosing to provide maintenance one their own must agree to and abide by the rules defined below, as well as provide root access to their computers on the net. Projects with their own professional computer support personnel will negotiate their own agreement with the computer support group.

The charge for connecting a computer to the network is $280. There is no charge for connecting a "network appliance" (a device which generally cannot be reprogrammed from the network, such as a printer or a network camera). There is no longer a distinction between "connect charges" and "support charges." It now costs the same to connect to the network whether or not one supports one's own machine(s).

For this amount, one can connect one's machine to the net. One also will be eligible for hardware support for PC-compatible hardware (including only labor, not parts), and for software support for a standard set of software on machines running Sun, Linux, and Windows.

The remainder of this message is a more-detailed discussion of the rules of computer usage and some general observations. Please read it before you sign the attached forms.

Please return all forms to Alan Koski, room 364. If you have any further questions about computing, please email Philip Pinto, ppinto@as.arizona.edu.

General Principles

The network is a shared resource upon which we all depend. The golden rule of computer etiquette is "do not use any more resources than you really need." While this no longer applies to individual computer's memory or CPU cycles, it applies to the network where the cost of expanding capacity is still significant.

If you are a heavy user of network resources, try to minimize your use of the network, or to make greatest use at times of the day which will lead to the least disturbance to others. If you are designing new systems, try to hide local network use behind a network firewall or switch.

A second golden rule is "keep security in mind." The Internet is under siege from people who would abuse our privacy, interfere with our work, and flood our mailboxes with trash. As fast as people can secure the network to known forms of attack, so other people are devising novel ways to cause problems.

Just as the physical security of property depends *e.g.* upon the cooperation of all in keeping the building locked after hours, so too does computer security rely upon everyone's cooperation. This is true even when "cooperating" means learning to do things in new and unfamiliar, or even less convenient, ways.

Changes (such as visitors, office moves, new equipment etc.) will be accommodated if sufficient advance notice is given to the CSG. Please do not plug your computer into a different location

without notifying the CSG *in advance*.

For all computer systems with multiple users (such as clusters or observing computers), users are obliged to be socially responsible in their use of disk, cpu, memory, and node resources.

All users are responsible for backing up their own data. At the present time, the CSG does not back up any data on a regular schedule.

The rules and policies listed here are in addition to any imposed by the University of Arizona or the State, some of which are listed on the University's CCIT website.

Appropriate Use

Computers may only be attached to the Steward network in connection with an official Observatory activity. The CSG *must* be told of any new computer's impending connection, including any visitor's computers, *before* they are connected.

Accounts on computers may only be given to officially-employed members of the Observatory or to collaborators in Observatory business. *All* accounts for non-Observatory employees must be registered with the CSG to avoid their being identified as illegal intruders. In particular, friends, relatives, and business associates may not be given accounts; this includes email, personal, and business accounts for family members. In addition, officially-sanctioned accounts may not be used for non-University business purposes, though use for personal Email and web access is generally acceptable. We have been audited and found in violation in the past, so we are forced to crack down on these activities.

Security

Security is essential to the predictable and reliable operation of a computer network. Maintaining the security of the network at Steward is therefore a primary task of the CSG; attention to security pervades all that they do.

In spite of this, the CSG cannot guarantee the uptime nor the security of the computing environment. It is therefore unwise to assume that the privacy of sensitive information is protected. New ways are discovered every day to gain unauthorized access to computers and to eavesdrop on networks. The privacy of information may also be compromised in more "legitimate" ways (see below).

It is similarly unwise to assume uninterrupted availability of the computing environment. Network access to/from Steward is often interrupted by events beyond the CSG's control including campus network maintenance and even errant back-hoes. In addition, the CSG may themselves shut down network access and/or services as needed to preserve the integrity of the computing environment. Reasonable effort will be made to notify users of interruptions, but timely warnings are not always possible. If uninterrupted service is critical to a project, it should make contingency plans in advance to deal with computing environment downtime. The CSG can help to design and implement such safeguards if given sufficient advance notice.

In order to maintain security, all networked equipment must be kept up-to-date with respect to security patches, service packs, etc. It is the responsibility of every computer user to ensure that this is done, either by requesting support from the CSG or by some other means of which the CSG is informed.

It is a sad fact that most software was and is still not designed with security in mind. A big part of ensuring security is thus the prohibition of many otherwise useful activities such software would enable. Computers at the Observatory may not run any services which are not previously authorized by the CSG. Prohibited services include, but are of course not limited to,

- unauthorized anonymous ftp sites

- dial-in modem service
- wireless networking access points
- all multicast network traffic
- DHCP servers
- DNS servers
- peer-to-peer file sharing (such as Kazaa, gnutella, and their ilk)
- telnet services

Any activity which can be seen as risking the security of, or worse, attempting to compromise, the network is similarly prohibited. Such activities include

- obtaining unauthorized root access to a computer
- sharing an account or a password with anyone
- port scanning
- packet sniffing
- denial of service
- password cracking
- altering the MAC address of equipment after is has been registered with the CSG
- altering the hardware or software configuration of a device one is not officially responsible for maintaining
- connecting a device to the network without an IP address
- using an IP address on a device to which it was not specifically assigned by the CSG
- moving a networked device (other than a laptop registered with the CSG) to a different physical location within the network

The CSG routinely scans computers on the Steward network for vulnerabilities, and monitors and logs network traffic to and from the Observatory. It may, at any time and without warning, disconnect or limit network access to any computer deemed to be at risk of compromise or exhibiting suspicious activity.

Email

A webmail service is now available to anyone in the Observatory. This allows one to use any IMAP-capable mail reading tool to retrieve mail, and in addition will allow access to mail through any web browser, without configuration, from anywhere in the world. This should make access to email easier from conferences, internet cafes, etc. More information about this new service will come in a separate message.

Unwanted email is rapidly becoming a problem of global proportions. Until governments enact and enforce anti-nuisance laws, we are all at the mercy of "spammers." No one can ensure that email

will be free of content that some may find undesirable or even offensive. At Steward, industry-standard tools are used to make a reasonable effort to identify spam and email messages with offensive content, but the CSG's scanners exist only as a convenience. In the escalating arms race between spammers and those attempting to identify spam, there is no guarantee that automated programs will properly identify content. It is certain that some offensive emails will be delivered without being labeled as such. Perhaps worse, it is also certain that some desired email will be delivered but incorrectly identified as spam.

The CSG employs *scanners*, which identify spam, not *filters*, which delete or redirect it. All mail which is not suspected of carrying a virus (see below) is delivered. When the CSG scanner identifies spam, it inserts message headers to indicate that the message *may* have unwanted content. Users are individually responsible for maintaining their own mail filters if they wish to avoid exposure to certain content. They may choose to make use of the keywords in CSG-inserted headers (for example `sssss`, or `PORN_01`), and they are further encouraged to create their own filters based on content found in the headers or body of emails (such as objectionable keywords or the existence of embedded images or URLs). The CSG section of the departmental website has instructions on how to do this.

All inbound email messages are also scanned for viruses. Messages believed to be infected or likely to expose a computer to a security vulnerability will have all or part of the message body or attachment removed. When this happens, users are sent an email notifying them that the message has been modified. In the event of a virus or worm which generates large numbers of virus warning messages, users are expected to create filters just as they would for spam messages if they wish to avoid seeing these warnings. As an additional defense against viruses, programs which read email must be configured not to run automatically any programs or scripts attached to email.

While the CSG will exercise due diligence in scanning email, it accepts no responsibility for damage or infection to computers by a virus which was not detected, nor for the modification of a message which was mistakenly identified as being infected.

Once again, a big part of maintaining security is the denial of useful capability in the face of security threats. Email to Steward email address groups and to destinations outside the Observatory is generally restricted to messages originating from Steward computers ("relaying" email is restricted). This will usually keep one from using one's email account to send email from remote locations using anything but the new web mail service.

Finally, the CSG provides no web-filtering service to control access to web pages or content that some users may find offensive or disconcerting. Users are responsible for exercising caution when clicking on links or typing URLs to ensure that they are not exposed to objectionable content. In general, users are expected to limit their use of the Internet to be in accordance with the University of Arizona's policies of appropriate use.

Privacy

We remind you of several aspects concerning privacy of information stored on computers. First, the University may assert the right to inspect files on any computer attached to a University network. As the law in this area is evolving, the University might well assert this right regardless of its actual right to do so, and regardless of whether it owns the computer. Information on your computer may be subject to a public records request made of the University. There is also the possibility that your computer may be the subject of a subpoena.

Backup copies of data are made from time to time. This may be for maintenance of an individual machine, as part of the regular Steward email service, or for because of some unanticipated problem. For this reason, data which you delete on your computer or the email server may not have fully disappeared. The equivalent of shredding files is very difficult to accomplish with computers, and

you should not rely upon deletion when you are required to destroy confidential information.

Finally, while CSG personnel will not deliberately read the contents of personal files on computer systems or read the content of email, they cannot guarantee that this will not happen inadvertently as a part of normal operation and maintenance of the system.

The moral: if you have information which you believe to be personal, private, or sensitive, you should carefully consider whether you want that information stored on your computer.

Steward Observatory Network Connection Agreement

The undersigned has read and agrees to all of the information and stipulations in the attached Operating Agreement, and is responsible for the computer equipment listed below.

Signature: _____

Name: _____

Account Number to charge: _____

Office Address: _____

Office Telephone: _____

Home Telephone (optional*): _____

Cellular Telephone (optional*): _____

* for notification in case of problems.

Computer name	Operating system	Computer location	Someone other than CSG will maintain this machine (name)