NOAO Backup Policy

1.0 Overview
This policy defines the backup policy for computers within NOAO.

NOAO maintains a large and growing body of data stored exclusively in electronic form. Much of these data are critical to the operation of NOAO, and it is clear that NOAO could suffer significant loss should an important set of data be permanently lost. Therefore, all data should be backed up. Cost and other practical issues may cause us to miss this ideal, hence NOAO must carefully consider the value of each dataset as we establish a backup plan.

2.0 Purpose
The purpose of the NOAO Backup Policy is to establish the rules for the backup and storage of electronic data currently stored on NOAO data systems.

This policy is designed to protect data in the Observatory to be sure it is not lost and can be recovered in the event of an equipment failure, intentional destruction of data, or disaster.

This policy is intended to ensure the integrity, availability, and confidentiality of NOAO's electronically maintained data, including but not limited to confidential, sensitive, or personally identifiable information. All NOAO units must ensure that planning is effected which ensures their ability to resume operation rapidly in the event of equipment failure, fire, flood, vandalism, or other causes of data loss.

Furthermore, each staff member should insure that his or her "personal" data kept on desktop or laptop computers are also backed up.

3.0 Scope
This policy applies to all NOAO departments, units, and staff that develop or create data in electronic format.

This policy applies to all equipment and data owned and operated by NOAO.

4.0 Policy
NOAO units maintaining datasets indispensable to the operation of NOAO must maintain effective, off-site backups. The standard to keep in mind is "business-continuity," or in less prosaic terms, to keep NOAO going in case the main building is reduced to a smoking crater.

In particular, the CIS Departments must maintain daily, off-site backups for systems necessary to network connectivity and operation including servers supporting email. WWW, name-service, remote access, etc. If possible, backup hardware should be stored at the offsite back-up location which can be quickly loaded with data and connected to pre-arranged, alternate connections to the Internet.

Other NOAO units with similar backup responsibilities are the ETS, CAS and HR departments and scientific projects (such as SDM and GONG) that maintain valuable datasets that the astronomical community depends on.

The CIS Departments also have a responsibility to maintain the lab and office computers that are used on a daily basis by staff. However, since the data stored on these computers is not obviously important to the observatory as a whole, the relevant back-up standard to be applied is "protect against equipment failure" rather than the "protect against a smoking crater disaster" standard applied above. The less rigorous standard allows weekly rather than daily backups and off-site storage of temporal subsets rather than the entire backup set. Furthermore, in most

cases, only the "system" portion of the data stored on these systems is backed up; the "data" portion is not.

Thus the onus for protecting data of importance to individual staff is placed squarely on the staff who own the data. While, because of cost and manpower limitations, the CIS Departments cannot back up all the data stored on staff desktop and laptop systems, CIS staff will consult with individual staff and units about back-up techniques and procedures ranging from department operated communal backup systems to external disks that an be loaded with back-ups and then stored under the bed at home.

5.0 Notes
- Datasets, documents, programs, etc. that are indispensable to the continued operation of the Observatory should not solely be stored on a laptop, desktop, office or lab computer. Rather, the data should be located on a server system with a rigorous (daily, off-site) backup policy.
- Sensitive data, including but not limited to personally identifiable information such as names, addresses and Social Security Numbers, should be encrypted both on the server and on the back-up media.
- NOAO units should take advantage of natural off-site backup sites offered by NOAO's geographical diversity: NOAO-Tucson can store (via on-line or off-line means) back-up datasets on Kitt Peak.
- Back-up procedures need to be documented, revised periodically and tested. A back-up that cannot be restored is no back-up at all!

6.0 Revision History
Created   July 10, 2006
Edited   July 12, 2006
Massively Revised   February 15, 2007
Edited   Februray 17, 2007
Revised   April 21, 2009