

# NOAO Information Sensitivity Policy

## 1.0 Purpose

The Information Sensitivity Policy is intended to help employees determine what information can be disclosed to non-employees, as well as the relative sensitivity of information that should not be disclosed outside of NOAO without proper authorization.

The information covered in these guidelines includes information that is either stored or shared via any means. This includes: electronic information, information on paper, and information shared orally or visually (such as telephone and video conferencing).

All employees should familiarize themselves with the information labeling and handling guidelines that follow this introduction. It should be noted that the sensitivity level definitions were created as guidelines and to emphasize common sense steps that you can take to protect NOAO Confidential information (e.g., NOAO Confidential information should not be left unattended in conference rooms).

*Please Note: The impact of these guidelines on daily activity should be minimal.*

Questions about the proper classification of a specific piece of information should be addressed to your manager. Questions about these guidelines should be addressed to the CIS Departments.

## 2.0 Scope

All NOAO information is categorized into two main classifications:

- NOAO Public
- NOAO Confidential

NOAO Public information is information that has been declared public knowledge by someone with the authority to do so, and can freely be given to anyone without any possible damage to NOAO. Examples of NOAO Public Information include employee names, email addresses and phone numbers (complete NOAO phone directories are not NOAO Public Information, however).

NOAO Confidential information contains all other non-public information. It is a continuum, in that it is understood that some information is more sensitive than other information, and should be protected in a more secure manner. Included are information that should be protected very closely, such as trade secrets, development programs, protected personnel information and other information integral to the success of the Observatory. Also included in NOAO Confidential is information that is less critical, such as telephone directories, general corporate information, etc., which do not require as stringent a degree of protection.

A subset of NOAO Confidential information is "NOAO Third Party Confidential" information. This is confidential information belonging or pertaining to another organization that has been entrusted to NOAO by that company under non-disclosure agreements and other contracts. Another example of NOAO Third Party Confidential information is telescope observing data that we hold in trust for our observers during the data proprietary period.

NOAO personnel are encouraged to use common sense judgment in securing NOAO Confidential information to the proper extent. If an employee is uncertain of the sensitivity of a particular piece of information, he/she should contact their manager

## 3.0 Policy

The Sensitivity Guidelines below provide details on how to protect information at varying sensitivity levels. Use these guidelines as a reference only, as actual NOAO Confidential

information may necessitate more or less stringent measures of protection depending upon the circumstances and the nature of the NOAO Confidential information in question.

### **3.1 Minimal Sensitivity**

If marking is desired, the words "NOAO Confidential" or "NOAO Proprietary" may be written or designated in a conspicuous place on or in the information in question.

The material may be accessed by NOAO employees and contractors with a business need to know. The material may be distributed within NOAO by Intranet sections of NOAO web sites, interoffice mail, electronic mail, and electronic file transmission methods. The material may be distributed outside NOAO via U.S. mail and other public or private carriers, electronic mail and electronic file transmission methods.

Keep material from view of unauthorized people; erase whiteboards, do not leave in view on tabletops. Machines storing material should be administered with security in mind: electronic information should have individual access controls where possible and appropriate.

Outdated paper information should be shredded; electronic data should be expunged/cleared. Reliably erase or physically destroy media.

### **3.2 Maximum Sensitivity**

If marking is desired, the words "NOAO Internal: Registered and Restricted" or "NOAO Eyes Only" may be written or designated in a conspicuous place on or in the information in question.

The material may be accessed only by designated individuals (NOAO employees or non-employees) with signed non-disclosure agreements. The material may be distributed within NOAO by direct delivery, signature required. The material may be distributed outside NOAO via direct delivery, signature required, by designated carriers.

Material stored electronically must be strongly encrypted. Machines storing material should be administered with strong security: individual access controls, physical security and strong encryption.

Outdated paper information should be shredded; electronic data should be expunged/cleared. Reliably erase or physically destroy media.

## **4.0 Terms and Definitions**

### **Expunge**

To reliably erase, overwrite or destroy data on a PC or Mac you must use a separate program to overwrite data. Otherwise, the PC's or Mac's normal erasure routine keeps the data intact until overwritten. The same thing happens on UNIX machines, but data is much more difficult to retrieve on UNIX systems.

### **Individual Access Controls**

Individual Access Controls are methods of electronically protecting files from being accessed by people other than those specifically designated by the owner. On UNIX machines, this is accomplished by careful use of the `chmod` command (use *man chmod* to find out more about it). On Mac's and PC's, this includes using passwords on screensavers, such as Disklock, and setting file access permissions specific to the operating system.

### **Encryption**

Secure NOAO Sensitive information in accordance with the NOAO Acceptable Encryption Use Policy. International issues regarding encryption are complex. Follow corporate guidelines on export controls on cryptography, and consult your manager and/or the CIS Departments for further guidance.

**Physical Security**

Physical security means either having actual possession of a computer at all times, or locking the computer in an unusable state to an object that is immovable. Methods of accomplishing this include having a special key to unlock the computer so it can be used, thereby ensuring that the computer cannot be simply rebooted to get around the protection. If it is a laptop or other portable computer, never leave it alone in a conference room, hotel room or on an airplane seat, etc. Make arrangements to lock the device in a hotel safe, or take it with you. In the office, always use a lockdown cable. When leaving the office for the day, secure the laptop and any other sensitive material in a locked drawer or cabinet.

**5.0 Revision History**

First Edition: March 15, 2007