NOAO Guidelines for Choosing a Good Password

It is easy to break into any account with a "bad" password. Such break-ins compromise the whole system, so all users must bear the resposibility of choosing good passwords.

The "best" passwords contain a mixture of uppercase letters, lowercase letters, numbers and punctuation (e.g. "lap5Dog%", "Whoosh?", "sUpEr8", "BIGpig!!"). The first characters of a memorable phrase in mixed case with additional numbers/punctionation would make a good password. For example, Mary had a little lamb: "5Mhall!"

- Long passwords are better than short passwords. Unfortunately, on our old Suns, characters beyond the 8th character are ignored. So use an eight character password on systems such as Tucson's Gemini and Ursa and 10 character passwords (or longer!) on modern Linux/FreeBSD systems (such as Tucson's Taurus and Crux) and on your Windows or Mac desktop and laptop.

- Any typeable characters are acceptable. So mix in some numbers and punctuation marks.

- The case of a letter is significant (e.g. "Sparc" and "sparc" are different).

- DO NOT use anything that can be found in any dictionary (e.g. "vorticity", "encomia", "Mervin" are obscure but they occur in common dictionaries so they should be avoided). This includes foreign words, slang, jargon, and proper names (e.g. "sayonara", "reboot", "Keohane").

- Avoid any names, words, numbers or abbreviations that can be found in your personal data (e.g. social security numbers, maiden names, name of relatives, any dates).

- Avoid passwords that can be "guessed" by knowing something personal about you. This includes nicknames, names of pets, names of significant others, anything from your favorite TV show (Trekkies beware!), your favorite book, lines from your favorite songs, etc. (e.g. "Picard", "NCC1701D", "Sparky").

- Avoid simple variants or permutations of any of the above (e.g. S's replaced by 5's, E's replaced by 3's, O's replaced by 0's, your name backwards or shifted, your login name repeated or backwards). Avoid using "text messaging" codes and leetspeak!

- DO NOT share your password or write it down anywhere accessible. System Administrators can give you a new temporary password if you forget it. You must change this immediately, using the UNIX passwd program or the Mac or Windows' password changing procedure.

- Change your password periodically: At least once a year, but avoid frequent changes lest you forget your password.

- Users who have accounts at other sites should use a unique password for each account, in order to contain the damage done if one of the passwords is compromised. Yes, I realize that this can drive a user crazy, but it is really important!

- If you are overwhelmed by the number of passwords you have to deal with, you might consider a password manager running on your desktop, laptop, or smartphone. In this case, you need only remember one password to decrypt all the passwords you need to

use (so make that one password a good one!). Examples of password managers are KeePass, LastPass, SplashID and 1Password.

- Many sites now ask for answers to "security questions" to be used for identity verification in case you have forgotten your password. Examples of such questions are "What is your Mother's Maiden Name?" or "What is the name of your High School?" While seemingly a good idea, the amount of data about you that lives on the Net can make these kinds of questions useless as a verification of identity. Just ask a prominent politician whose Yahoo email account was hacked into. The best advice we can give you is to lie (but to preserve your sanity, lie consistently!).

- Do not use any passwords used in this document!

Revision History
First Edition: March 15, 2007
Revised: May 19, 2010