

SNAS Beta System Rules of Behavior

The Office of Management and Budget (OMB) Circular A-130, Appendix III, Security of Federal Automated Information Resources requires that "Rules of Behavior" be established for each general support information technology (IT) system and major application processing government information. The "Rules of Behavior" delineated below pertain to all persons who utilize the Space Network Access System (SNAS) which is an IT resource of the Space Communications Program of NASA's Goddard Space Flight Center (GSFC).

As a customer and user of NASA's GSFC IT resources, I understand that I am responsible for adhering to the rules listed below:

1. Your SNAS account is only for official use in performing your assigned duties.
2. You must protect all software on the SNAS Client in accordance with NASA, contractor, international partner, or best security practices of government and industry.
3. You must use licensed software in accordance with the license.
4. You agree to not add any software without authorization and a proper license.
5. You agree not to download or add software from untrusted sources.
6. You are not allowed to reverse engineer or modify the SNAS Software.
7. Any unauthorized penetration attempt, unauthorized system use, or virus activity will be reported to your supervisor, project manager, system administrator and IT Security Officer.
8. You consent to monitoring and security testing to ensure proper security procedures and appropriate usage are being observed.
9. You must not use the IT resources for fraudulent, harassment or obscene messages and/or materials.
10. When you no longer need SNAS in your official duties, you must notify appropriate responsible parties and make no further attempt to access SNAS.
11. You must erase fixed media prior to transferring the SNAS Client or designating the SNAS Client for excess.
12. You are not allowed to tamper with another user's account, files, or processes without the other user's express permission.
13. You are not allowed to use SNAS system resources for personal purposes or other unauthorized activities.
14. You are not allowed to transfer or share Login IDs and/or passwords for any reason.
15. Group ID, group passwords, and group passphrases are prohibited.
16. Passwords:
 - a. will be a minimum of 8 alphanumeric characters with at least one (1) character from each of these categories: lower case alpha, upper case alpha, numeral and special character;
 - b. will not consist of personal ID data;
 - c. will not be a word appearing in an English language or foreign language dictionary;
 - d. will not be easily guessable;
 - e. will be changed at least every 90 days;
 - f. will not be reused within a 180 day period;
 - g. will be memorized and not written down;
 - h. and will not be stored in keyboard macros, script, or batch files.
17. Passphrases:
 - a. A passphrase is a string of words and characters that you type in to authenticate yourself. Passphrases differ from passwords only in length. Passwords are usually short - 8 to 16 characters. Passphrases are usually much longer - up to 100 characters or more. A passphrase should be known only to you, long enough to be secure, hard to guess -- even by someone who knows you well, and easy for you to remember and type accurately. In addition to the restrictions for passwords listed previously, passphrases:
 - b. will be a minimum of 20 characters in length (including spaces);
 - c. will be a minimum of 4 words, i.e., 4 groups of characters separated by spaces;
 - d. will be at least 6 unique characters (characters with only 1 occurrence in passphrase);
 - e. will have at least one character from each of the four groups: lower case alpha, upper case alpha, numerals and special characters including punctuation characters;
 - f. will not reuse the same passphrase within a 2 year period;
 - g. will have cycled through 5 passphrases before reuse;
 - h. can not be cached.

SNAS Beta System Rules of Behavior

- 18. Internet Access:
 - a. When the Internet is used to access SNAS, the SNAS Client will utilize up-to-date anti-virus software, up-to-date anti-spyware software, a properly configured firewall and other reasonable measures to protect against compromise of the system.
- 19. Mobile access:
 - a. Laptops will be stored in a secure location when not in use.
 - b. SNAS data stored as local files will be encrypted.
 - c. Precautions will be taken to prevent snooping by unauthorized individuals.

Acknowledgement Statement

Unauthorized use of the computer accounts and computer resources to which I am granted access is a violation of Section 799, Title 18, U.S. Code; constitutes theft; and is punishable by law. I understand that I am the only individual to access these accounts and will not knowingly permit access by others without written approval. I understand that my misuse of assigned accounts, and my accessing others' accounts without authorization is not allowed. I understand that this/these system(s) and resources are subject to monitoring and recording. I further understand that failure to abide by these provisions may constitute grounds for termination of access privileges, administrative action, and/or civil or criminal prosecution.

Requester's Signature

Date Signed

Supervisor's or Project Manager's Signature

Date Signed

Please Print

User's Full Name:	Phone Number:										
Project or Mission:											
Employer/Affiliation/Organization/Code:											
Location or Address:											
Email Address:											
Supervisor or Project Manager:	Phone Number:										
FQDN/IP Address(es):											
Citizenship of Requestor											
Role/Level of Privilege (Check all that apply):	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 20px; text-align: center;"><input type="checkbox"/></td> <td>Mission Manager</td> </tr> <tr> <td style="text-align: center;"><input type="checkbox"/></td> <td>Mission Scheduler/Planner</td> </tr> <tr> <td style="text-align: center;"><input type="checkbox"/></td> <td>Mission Controller</td> </tr> <tr> <td style="text-align: center;"><input type="checkbox"/></td> <td>Mission Support</td> </tr> <tr> <td style="text-align: center;"><input type="checkbox"/></td> <td>Mission Observer</td> </tr> </table>	<input type="checkbox"/>	Mission Manager	<input type="checkbox"/>	Mission Scheduler/Planner	<input type="checkbox"/>	Mission Controller	<input type="checkbox"/>	Mission Support	<input type="checkbox"/>	Mission Observer
<input type="checkbox"/>	Mission Manager										
<input type="checkbox"/>	Mission Scheduler/Planner										
<input type="checkbox"/>	Mission Controller										
<input type="checkbox"/>	Mission Support										
<input type="checkbox"/>	Mission Observer										

Fax completed form to the SNAS System Administrator: 301-286-1727