

Personal Information and Rules of Conduct Document

This document fulfills the personal information requirement of NPG2810.1 Section 4.7.7 which states:
System Administrators shall require an Account Request Document for each user who requests access to a multiuser IT system.

Personal Information

Name, office mailing address, office phone, office e-mail address

Name: _____

Address 1: _____

Address 2: _____

City: _____

State, ZIP: _____

Phone: _____

E-Mail: _____

Citizenship

U.S. Citizenship: Y / N (circle one)

If not a U.S. Citizen, please complete the following:

Citizenship Status: _____

ex. Permanent Resident Alien or Foreign National, etc.

From what country will this account be accessed: _____

Affiliation

Organization Code/Company Name/University Name or other Affiliation Identification:

Non-government employees:

Identification of the official relationship of the requester to NASA:

ex. grant, Memorandum of Understanding, contract, or other work agreement, etc.

Acknowledgement of Use/Misuse

By signing below, the user is indicating that he/she has read, understands and will comply with the following 3 pages which describe official business use and acceptable use for NASA computer systems. These pages are the statements of NPG2810.1 Sections 4.8.2 - 4.8.4, and 4.9.

By signing below, the user is indicating that he/she has read, understands and will comply with the next 2 pages which describe the Rules of Behavior for Code 920 administrated systems.

The following statement is required by NPG2810.1 Section 4.7.7 Figure 4-8 and is also acknowledged by the user's signature below.

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 criminal prosecution.

Printed Name: _____

Signature: _____ Date: _____

6/2/2000

NPG2810.1 Computer Systems Rules of Conduct

4.8.2. Official Business Use of Government Resources

NASA provides computer systems for the purpose of transacting official business. The following sections provide guidance on what is considered official business use, what is not considered official business use, and what use may be considered acceptable use with proper approval.

4.8.3. Official Business Uses

4.8.3.1. Official business broadly includes any computer processing that is required as part of the job. Official business includes, but is not limited to, the performance of NASA work-related duties in position descriptions, professional training and class work, work covered under grant agreements with NASA, tasks directed via NASA contracts, agreements with international partners, Center-authorized activities, and support activities related to NASA contract tasking.

4.8.3.2. With the concurrence of appropriate Center management, some less formal activities may be authorized. Authorization for such activities should be documented by management and may include, but not be limited to, the following:

- a. Work-related events, such as a technical symposiums, classes, and presentations.
- b. Activities sponsored by the Center, such as child care center and carpooling activities.
- c. Events and activities specific to a particular NASA or Center organization.
- d. Center-sanctioned activities, such as blood drives, sanctioned clubs, and organizations.

4.8.3.3. Management may permit some infrequent personal use of electronic mail. When communication cannot reasonably be made during non-business hours, employees may exchange brief messages with such persons or entities as the following:

- a. Spouse or dependent.
- b. Someone responsible for the care of a spouse or dependent.
- c. State and local government agencies on personal matters.
- d. Medical care providers.
- e. Dentists.
- f. Users may also use electronic mail in emergency situations.

4.8.4. Other Permissible Uses

4.8.4.1. Because there is no measurable cost, some limited personal use of Internet services, such as the World Wide Web and electronic mail, is permitted, provided it does not interfere with the employee's work or the work of others. Extreme care must be taken regarding content matter. Under no circumstances is it permissible to access or download material that would create a hostile or offensive work environment, such as racist or sexually explicit material. Use must be kept to brief periods when it can reasonably be assumed that the employee is in a nonduty status, such as during lunch breaks.

4.8.4.2. Some uses of NASA computer systems are clearly outside the boundaries of official business and permissible use. Prohibited uses of NASA's IT resources include using systems to do the following:

- a. Maintaining or conducting an outside business.
- b. Monitoring network traffic (e.g., run a sniffer); access IT resources; or copy data, files, or software without prior authorization. (Activities for which prior authorization is assumed include performing defined job duties, copying information that is intended to be copied, and doing work that has been approved by the Center IT Security Manager.)
- c. Participating in Chat Rooms, News Groups, or similar activities where the posting will be seen by the public. Use of the NASA Internet address of "nasa.gov" is a representation of the Agency, analogous to the use of NASA letterhead in which the opinions expressed reflect on NASA.
- d. Advertising goods or services for sale for monetary or personal gain.
- e. Sending chain letters, personal mass mailings, hoaxes, or harassing messages.

4.8.4.3 Users should be particularly careful about using NASA computer systems in any way that could be interpreted as intending to influence any member of Congress to favor or oppose any legislation or appropriation. If the offender is an officer or employee of the United States, such an act may fall under a provision of Title 18 U. S. Code, Section 1913, "Lobbying with appropriated monies," which carries severe penalties upon conviction. If there are any questions about any aspect of this provision of law, contact your Center's Office of Chief Counsel for advice and assistance.

4.9. Software Usage

4.9.1. Overview

All users of NASA resources must comply with the terms of any license agreement for any software that NASA provides. It is usually illegal in the United States and most other countries to make or distribute copies of copyrighted material without authorization from the copyright holder. The NASA OIG, line managers, and other authorized individuals occasionally audit U.S. Government-owned equipment for the presence of unlicensed software. Each user is responsible for reading and complying with the terms of the license agreement that accompanies software.

4.9.2. Usage Guidelines by Software Type

The following are guidelines for appropriately using software:

- a. Public Domain Software--Some software authors choose to make their software publicly available under terms that the author may specify. This public domain software may be used on NASA computers at the option of the line manager.
- b. Shareware--Shareware is software that is available for a trial period at no cost. Users who wish to continue using shareware after the trial period may then be required to pay a license fee. Shareware is permitted on NASA computers at the option of the line manager, but the license fee must be paid.
- c. Software Use at Home--Many users have workstations at home where they perform job-related work. Some software licenses accommodate use at home as well as at work. Some licenses may even permit personal home use of Government-purchased software. NASA allows users to make any legitimate use of a

Government-purchased software package that is consistent with the license agreement. The burden is on the user to understand and to comply with that agreement.

d. Inspection of Imported Software for Malicious Code--All software entering the NASA community is called "imported software." Before being installed on any NASA-owned computer, all imported software must be approved by the responsible line manager. Each line manager may have a slightly different approval process, but all approval processes must include a check for the presence of malicious code, such as viruses, trap doors, and trojan code. Diskettes that users bring from home and diskettes that they bring back from travel have in the past been fertile sources of computer viruses. The use of imported software is permitted, but the user must take responsibility for examining it for the presence of malicious code before installing it. NASA and its immediate contractor community are required to have a process in place to inspect imported software. For more assistance, contact your organizational CSO.

Rules of Behavior for the NASA GSFC Code 920 Automated Information Systems

These guidelines are for the use of the information technology (IT) resources operated within the Automated Information Systems in the Laboratory for Terrestrial Physics (Code 920) of NASA's Goddard Space Flight Center. The purpose of these guidelines is to increase individual awareness and responsibility and to ensure that all users use the Division's IT resources in an efficient, ethical, and lawful manner.

- (1) I will use only those IT resources which I am authorized to use. If I require any additional privileges or resources, I will contact my system administrator/group leader for these.
- (2) I will not use more than my fair share of IT resources. To the best of my ability, I will monitor my use of disk space, memory, network bandwidth, and CPU time; and I will not allow my processes to deny other users' legitimate access to these resources.
- (3) I will not attempt to bypass appropriate access controls, including login controls. I shall not attempt to access any data or programs contained on systems for which I am not authorized nor have consent of the data or program owner.
- (4) I am responsible for protecting and maintaining, to the best of my ability, any information used or stored in my accounts. As a part of this protection, I acknowledge my responsibility for knowing the retention period of information on backup tapes maintained by the sysadmin for my system and will maintain separate backups of all files and directories that must be saved beyond the nominal retention period of system backup tapes.
- (5) I will not divulge account access procedures to any unauthorized user.
- (6) I will use only accounts (userid/passwords) for which I am authorized.
- (7) I understand that good, secure passwords are required on all Code 920 systems. I understand that passwords should be at least six characters long, should contain at least one non-alphabetic character, and should never be a word, proper name, or standard abbreviation.
- (8) I shall not make or use unauthorized copies of copyrighted software, except as permitted by law or by the owner of the copyright.
- (9) When I no longer need access to these IT resources, I will notify my system administrator/group leader and make no further attempt to access these resources.
- (10) I am required to report all observed compromises of IT security (viruses, unauthorized access, theft, inappropriate use, etc.) to the Data Processing Computer Security Official, DPI-CSO, for Code 920.
- (11) I understand that these IT resources are the property of the United States Government, and that the Government reserves the right to conduct monitoring and security testing to ensure proper security procedures and appropriate usage of these resources.
- (12) Electronic communications facilities (such as e-mail, netnews, and the world-wide web) are for authorized Government use only. I agree not to use Code 920 IT resources for fraudulent, harassing, or obscene messages and/or materials. Additionally, I shall not send, retain, nor proliferate any such material on any Government systems, except as required by appropriate authorities to document such messages and/or materials.

(13) I will get a property pass from the property custodian before I remove any government-owned equipment from the premises. Such equipment is to be used for Government-related business only.

(14) I understand that all data and programs which are not factory-installed must be removed from my computers' disks before they are excessed.

(15) I understand that other organizations within Goddard Space Flight Center and within NASA may provide access to IT resources, such as the CNE's Annex dial-in lines, which are not under the control of Code 920.

I understand that I must be aware of and abide by those organizations' usage guidelines for access to their resources.