

Acceptable Use Statement for NAS Systems Division Computing Resources

The following document outlines guidelines for use of the computing systems and facilities located at or operated by the Numerical Aerodynamic Simulation (NAS) Systems Division at NASA Ames Research Center. The definition of NAS Systems Division and computing facilities will include any computer, server or network provided or supported by the NAS Systems Division. Use of the computer facilities includes the use of data/programs stored on NAS Systems Division computing systems, data/programs stored on magnetic tape, floppy disk, CD ROM or other storage media that is owned and maintained by the NAS Systems Division. The "user" of the system is the person requesting an account (or accounts) in order to perform work in support of the NAS program or a project authorized for the NAS Systems Division. The purpose of these guidelines is to ensure that all NAS users (scientific users, support personnel and management) use the NAS Systems Division computing facilities in a effective, efficient, ethical and lawful manner.

NAS accounts are to be used only for the purpose for which they are authorized and are not to be used for non-NAS related activities. Unauthorized use of a NAS account/system is in violation of Section 799, Title 18, U.S. Code, and constitutes theft and is punishable by law. Therefore, unauthorized use of NAS Systems Division computing systems and facilities may constitute grounds for either civil or criminal prosecution.

In the text below, "users" refers to users of the NAS Systems Division computing systems and facilities.

1. The NAS Systems Division computing systems are unclassified systems. Therefore, classified information may not be processed, entered or stored on a NAS Systems Division computing system. Information is considered "classified" if it is Top Secret, Secret and/or Confidential information which requires safeguarding in the interest of National Security.
2. Users are responsible for protecting any information used and/or stored on/in their NAS accounts. Consult the NAS User Guide for guidelines on protecting your account and information using the standard system protection mechanisms.
3. Users are requested to report any weaknesses in NAS computer security, any incidents of possible misuse or violation of this agreement to the proper authorities by contacting NAS User Services or by sending electronic mail to *security@nas.nasa.gov*.
4. Users shall not attempt to access any data or programs contained on NAS systems for which they do not have authorization or explicit consent of the owner of the data/program, the NAS Division Chief or the NAS Data Processing Installation Computer Security Officer (DPI-CSO).
5. Users shall not divulge Dialup or Dialback modem phone numbers to anyone.
6. Users shall not share their NAS account(s) with anyone. This includes sharing the password to the account, providing access via an .rhost entry or other means of sharing.
7. Users shall not make unauthorized copies of copyrighted software, except as permitted by law or by the owner of the copyright.
8. Users shall not make copies of system configuration files (e.g. */etc/passwd*) for their own, unauthorized personal use or to provide to other people/users for unauthorized uses.
9. Users shall not purposely engage in activity with the intent to: harass other users; degrade the performance of systems; deprive an authorized NAS user access to a NAS resource; obtain extra resources, beyond those allocated; circumvent NAS computer security measures or gain access to a NAS system for which proper authorization has not been given.
10. Electronic communication facilities (such as Email or Netnews) are for authorized government use only. Fraudulent, harassing or obscene messages and/or materials shall not be sent from, to or stored on NAS systems.
11. Users shall not down-load, install or run security programs or utilities which reveal weaknesses in the security of a system. For example, NAS users shall not run password cracking programs on NAS Systems Division computing systems.

Any noncompliance with these requirements will constitute a security violation and will be reported to the management of the NAS user and the NAS DPI-CSO and will result in short-term or permanent loss of access to NAS Systems Division computing systems. Serious violations may result in civil or criminal prosecution.

I have read and understand the NAS Systems Division computing systems Use Ethics Statement for use of the NAS computing facility and agree to abide by it.

Requestor's Signature

Date