

Table of Contents

<u>Data Storage Policies</u>	1
<u>Quota Policy on Disk Space and Files</u>	1
<u>Acceptable Use Statement</u>	3
<u>SUID/SGID Scripts</u>	5

Data Storage Policies

Quota Policy on Disk Space and Files

Filesystems on Pleiades, Columbia, and Lou have quotas: limits on the total disk space occupied by your files, and limits on how many files (represented by inodes) you can store, irrespective of size. For quota purposes, directories count as files.

Quota Hard and Soft Limits

There are hard limits and soft limits on quotas. Hard limits can never be exceeded. Any attempt to use more than your hard limit will be refused with an error. Soft limits can be exceeded temporarily, for a grace period of 14 days. If you remain over your soft limit for more than 14 days, the soft limit is enforced as a hard limit, in which case you will not be able to add or extend files until you get back under the soft limit. Usually, this means deleting unneeded files or copying important files elsewhere (such as [the Lou mass storage system](#)) and then removing them locally.

Table of Quotas on Columbia, Pleiades, and Lou

Default Quotas on Disk Space and Files			
	Columbia	Pleiades	Lou
\$HOME	NFS	NFS	XFS
Space: soft	4 GB	8 GB	none
Space: hard	5 GB	10 GB	none
Inode: soft	none	none	250,000
Inode: hard	none	none	300,000
/nobackup	CXFS /nobackup1[e-h] /nobackup2[a-j]	Lustre /nobackupp[1-6]	N/A
Space: soft	200 GB	500 GB	N/A
Space: hard	400 GB	1 TB	N/A
Inode: soft	25,000	75,000	N/A
Inode: hard	50,000	100,000	N/A

Email Warnings and Consequences

It is expected that you will exceed your soft limits as needed. When you exceed your soft limit you will begin getting daily emails to inform you of your current disk space and how

much of your grace period remains. During the grace period, these emails are intended to be informative and not a demand to immediately remove files. However, if you are still over your soft limit on Columbia and/or Pleiades after 14 days, your batch queue access will be disabled. On Lou, after 14 days of exceeding your soft limit, you will be unable to archive files until you have reduced your use to below the soft limit.

Disabled Batch Access on Pleiades/Columbia

If an account no longer has batch access to Columbia and/or Pleiades, all data from that system should be moved off within 7 days (or sooner if the other projects need the space).

If an account has been disabled for more than 14 days, its Columbia and/or Pleiades data will be moved to the archive host, Lou, and kept there for 6 months before removal, unless the project lead requests having the data moved to another account.

Disk File Quotas on Lou

There is no quota for file space on *Lou1* or *Lou2* because data that does not fit on disk is written to tape. There is a quota on the number of files you can store. Currently there is a soft limit of 250,000 files and a hard limit of 300,000 files.

The maximum size of a file moved to Lou should not exceed 30% of the size of your home filesystem on Lou. If you need to archive files larger than this, please contact the NAS Control Room at support@nas.nasa.gov for assistance.

Changing Your Quotas

If an account needs larger quota limits, send an email justification to support@nas.nasa.gov. This will be reviewed by the HECC Deputy Project Manager, Bill Thigpen, for approval.

Acceptable Use Statement

This document gives the requirements for use of the computing systems, resources and facilities located at and/or operated by the NASA Advanced Supercomputing (NAS) Division at NASA Ames Research Center.

As a user of the computing systems, resources and facilities located at and/or operated by the NASA Advanced Supercomputing (NAS) Division at NASA Ames Research Center, I agree to the following and understand that failure to abide by these provisions may constitute grounds for termination of access privileges, administrative action, and/or civil or criminal prosecution:

1. NAS accounts are to be used only for the purpose for which they are authorized and are not to be used for non-NASA related activities.
2. Unauthorized use of the computer accounts and computer resources to which I am granted access is a violation of Federal law; constitutes theft; and is punishable by law (Section 799, Title 18, U.S. Code). 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 sharing passwords with other people, even on the same project, is prohibited. 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 and I will have no expectation of privacy in my use of these systems.
3. I am responsible for using the computing systems, resources and facilities in an efficient and effective manner. I understand that account deactivation will result after 60 days of non-use and data will be deleted after 90 days unless my project or I make arrangements with the NAS User Services to preserve my data.
4. I understand that these computing systems are unclassified systems. Therefore, processing and storing classified, or other information that requires safeguarding in the interest of National Security, is prohibited.
5. I understand that these computing systems are categorized as moderate according to FIPS 199, therefore processing and storing information that is categorized as high according to FIPS 199 and NIST SP 800-60 is prohibited.
6. I understand that I am responsible for protecting any information processed or stored in my accounts and will take appropriate precautions to protect Sensitive But Unclassified information (e.g., proprietary information or information subject to International Traffic in Arms Regulations or Export Control Regulations) which may include encrypting the data to provide protection that goes beyond the standard OS protection provided by the computing systems.
7. I understand that I shall not engage in activities that compromise or weaken the security of the NAS systems or have been identified as prohibited and high-risk practices by the NAS Security Team. These activities include but are not limited to keeping unauthorized world-writable directories, running password cracking programs, downloading or introducing malicious software, running unauthorized P2P and VOIP software and copying or making available system and password configuration files to others.

8. I understand that I shall not make copies of copyrighted software, except as permitted by law or by the owner of the copyright.
9. I understand that I shall not attempt to access any data or programs contained on systems for which I do not have authorization or explicit consent from the owner of the data/program, the NAS Division Chief or the NAS Computer Security Official.
10. I understand that I am required to report any security weaknesses in the systems or any IT security incidents including misuse or violation of this agreement, to the NAS User Services, support@nas.nasa.gov, or to the NAS Security Team, security@nas.nasa.gov.
11. I understand that I am required to access the NAS computers only from remote systems that are safe from malicious programs and activity.
12. I understand that I will be required to complete the NASA mandatory Basic IT Security Training available at: <http://saturn.nasa.gov/>. (Note: Additional details are available from NAS User Services.)
13. If applicable, I further agree to abide by the provisions NASA NPD 2540.1G regulating privileges and responsibilities of NASA employees and contractors.

SUID/SGID Scripts

Users are prohibited from creating and using privileged SUID and/or SGID scripts under their home, scratch, `/nobackup`, and `/tmp` filesystems.

SUID scripts (that is, with permission `u+s`) and SGID scripts (with permission `g+s`) could allow someone (other than the owner) to gain unauthorized access to users' files, posing a security hazard.

WARNING: The high end computing systems at the NAS facility are configured to disable the execution of any SUID/SGID shell scripts.