

ACCESS AND USE POLICY FOR THE "AZNAVOUR" SUPERCOMPUTER

1) General Provisions

The following Rules set out the conditions for access to, and the method of using, the computing facilities of the "Aznavour" supercomputer, namely the compute nodes, the Slurm job scheduler, the Lustre parallel file system (/scratch), the NFS network storage (/home, /shared), the login nodes, the visualisation (viz) nodes, and the InfiniBand network.

The Rules apply to all users, including staff, graduate students, undergraduate students, and external collaborators. Access is provided within the context of a registered project.

The project lead is responsible for the intended use of allocated resources by all participants in their project.

2) Conditions for Granting Access

- Access is granted following the submission and approval of an "Application for Access to Computing Resources".
- Each project has a fixed duration (a phase of at most 12 months) and a budget for resources; it can only be renewed following a re-submission and obtaining approval.
- Resources are provided for scientific, engineering, and educational purposes. Commercial use is possible only under a separate agreement.
- Users must immediately inform the administrators of any change in their contact information or of their place of employment or study.

3) Accounts and Authentication

- Accounts are personal. Users must not share account credentials or private SSH keys or permit others to use their accounts.
- Access to the nodes is carried out solely through SSH using key-based authentication, password logins being disabled. The private keys are kept only by their owner.
- Secure protocols only are allowed (SSH, SFTP, SCP); the use of Telnet, unencrypted FTP, or any other plaintext data-transfer protocols is forbidden.
- A single user is allowed to take part in several projects using one account, but it is not permitted to create multiple accounts for the same individual.

4) Rules for Using Computing Resources

- **Login nodes** are designated for job preparation, compilation, and lightweight tasks. CPU- or memory-intensive computations are prohibited on login nodes. Idle sessions may be terminated after the set limit, and the number of simultaneous sessions is restricted.
- **Compute nodes** (compute[001–612]) are accessed exclusively through the Slurm scheduler. Direct access to compute nodes outside the Slurm scheduler is prohibited.
- **Visualization nodes** (armenia-viz01/02) are for interactive visualization using OpenGL or remote 3D desktop via VNC. They are not intended for GPU computation.

5) Data Storage and Management

- The **/home (NFS)** partition contains home directories with code, configuration files, and small results; it has been backed up and is not designed for intensive parallel I/O.
- The **/scratch (Lustre)** directory is the area used for parallel I/O. It is not backed up and data is automatically deleted in accordance with the retention policy. It is important to export your results promptly.

It should be avoided to carry out a large-scale generation and processing of a multitude of small files on the parallel file system since this will degrade the performance for all users.

Users are required to adhere to their assigned disk quotas, since going over a quota can result in job submissions being blocked.

6) Prohibited Actions

- Trying to gain unauthorized access, such as by guessing passwords or keys, scanning networks and systems, or exploiting vulnerabilities.
- Avoiding the job scheduler or ignoring set resource limits.
- Selling or giving your assigned compute time to others.
- Using resources for cryptocurrency mining or any tasks not related to the main purpose.
- Hosting, storing, or processing illegal content, or violating software copyright or license terms.
- Doing anything on purpose that harms the system's performance or disrupts other users.

7) Security and Incident Response

- If a key or account is suspected to be compromised, the user must immediately notify ANSCC administrators and replace the key via a secure channel.
- An account with no login activity for more than 180 days may be automatically disabled.
- ANSCC administrators will never ask users for passwords or private keys.
- Users are responsible for the security of their own data and working environment and must follow standard information-security practices.

8) Liability and Sanctions

Violating these Rules may lead to suspension or termination of user access. Systematic violations may result in loss of access for the entire project. Research teams that do not submit a project report may be barred from using the computational resources of the “Aznavour” Supercomputer for a specified period. The project lead is accountable for all project participants.