

Centre of Operations of the Slovak Academy of Sciences, SAS
Computing Centre

National Supercomputing Centre, non-profit organization

Terms of Use of High-Performance Computing Facilities

The Centre of Operations of the Slovak Academy of Sciences, SAS Computing Centre, in collaboration with the National Supercomputing Centre, operates high-performance computing infrastructure and provides access to it. Access to computing resources is available to users from academic, public, and private sectors according to the currently valid Rules for Access.

Information and manuals are available on the userdocs.nsc.sk website.

This document defines rules ensuring efficient, secure, and fair utilization of computing resources. We require all users to adhere to these rules. In case of any violations, we will notify the project leader; in the case of repeated or serious breaches, it may lead to the suspension or termination of computing tasks and, in extreme cases, the cancellation of user accounts and legal actions.

Access to Computing Resources and Their Secure Use

1. A user with a specific affiliation may have only one account, which must not be shared with anyone else. Users are obligated to protect and keep passwords, SSH keys, and other security elements secure. If a user suspects that their password has been compromised or their account is at risk, they must promptly report it to helpdesk@nsc.sk.
2. In case of suspicion of any security breach related to any of the HPC systems, the user must promptly report it to helpdesk@nsc.sk.
3. Changing or bypassing access controls and performing any actions beyond the assigned permissions is prohibited.
4. Computing capacities may be used strictly for approved projects, and their misuse for personal purposes is prohibited.
5. The so-called login nodes may only be used for submitting computing tasks to the batch system, software development (editing, compilation, etc.), and short, computationally non-intensive processes. Computationally intensive tasks (memory, CPU, I/O read and write) can only be executed through the batch system.
6. A user may be part of multiple projects, to which they are assigned based on the project leader's request.
7. The project leader is responsible for the implementation of the approved project and may request the assignment of users to this project. The project leader is obliged to provide detailed information

about the project's results upon request and prepare a final report, or other reports and surveys upon the operator's request. The project leader is also responsible for presenting the project at the annual "HPC-SK Conference" in the form of a poster or presentation.

8. The project leader must report any changes to the project's team (e.g., users who are no longer participating in the project).

9. The project leader is responsible for assigning all project outputs (e.g., scientific publications) to the database through the user portal.

10. The project leader is obliged to acknowledge the results and data obtained using the computing resources of the Computational Centre of the Slovak Academy of Sciences by including the following statement:

"The research (or part of it) was carried out using the computational infrastructure acquired in the project National Competence Centre for High-Performance Computing (project code: 311070AKF2) funded by the European Regional Development Fund, EU Structural Funds, Informatization of Society, Operational Programme Integrated Infrastructure 2014-2020."

11. All users are required to report any changes to their personal and contact details (email, phone number, relationship to the employer, etc.) through the user portal or at helpdesk@nsc.sk.

Software Equipment

1. The operator provides a standard software environment with common libraries and compilers, as well as several software packages with free licenses, available to all users as part of access to the HPC infrastructure.

2. Users can use their own software tools if obtained in accordance with the relevant licensing conditions.

3. All software packages must be installed and used in compliance with the respective license.

4. Users must not intentionally introduce or use malicious software, including but not limited to viruses, worms, ransomware, etc.

5. Reverse engineering of information and software without authorization is prohibited.

Handling of Data

1. Storage capacities may be used strictly for approved projects, and their misuse for personal purposes is prohibited.

2. Users have access rights only to data they own or have been granted permission to access and manipulate.

3. Users are solely responsible for data stored within the allocated storage capacities.

4. Users are also responsible for the security of data processed or stored on the operator's systems. In case of working with sensitive data, the operator recommends anonymization or the use of encryption tools.

5. The operator performs data backups created and stored by users at regular intervals only to a limited extent. The operator recommends users to regularly back up their data; in case of data loss, the operator is not responsible for their recovery.

The operator reserves the right to store and process personal data of users in accordance with the Principles of Personal Data Protection.