

Acceptable Use Policy of HPC Resources at IT4Innovations

Introduction

IT4Innovations national supercomputing center (IT4I) provides computational resources. These resources include: core hours, license hours, data storage capacity as well as network connectivity and human expertise. Purpose of this document is to define the rules and terms governing acceptable use of these resources, including access, utilization and security of the resources and data.

Definition of terms

- **Batch system:** The batch system is used to schedule and execute computational tasks of the users and to allocate computational resources necessary to complete these tasks. Currently, the PBS Pro system is used at IT4I.
- **HPC systems:** Collection of systems dedicated to High Performance Computing. These include the IT4I computational cluster and its support infrastructure.
- **IT4I:** IT4Innovations national supercomputing center
- **Passphrase:** A password or entire phrase (sentence) used to protect the private key. The passphrase is used to encrypt and decrypt the key. It should be kept secret at all times and should not be disclosed to anyone.
- **Project:** A set of activities and efforts to achieve aims and objectives approved by IT4I access evaluation committee. Computational resources at IT4I are allocated to Projects. Projects are given unique identifier, which is used to associate the Project with Users and computational resources.
- **Primary Investigator (PI):** A person responsible for executing the Project in order to achieve approved aims and objectives.
- **Private key:** A file containing the private part of the key pair. The private key along with its public part is used to encrypt information exchanged during authentication to IT4I HPC systems and is essential to obtain access. The key must be protected by encryption, so that it is useless in the case it falls into unauthorized hands.
- **System password:** A central password providing authentication of Users to various services at IT4I. It should be kept secret at all times and should not be disclosed to anyone.
- **User:** A person holding user account at IT4I.
- **User account:** Account assigned to user to access and utilize the computational resources provided by IT4I.

Computer use

Computers, software, and communications systems provided by the IT4I are to be used for purposes associated with and within the scope of the approved Project. The use of IT4I resources for personal or non-related activities is prohibited. Any misuse or unauthorized access is prohibited, and may be subject to criminal or civil proceedings.

User accounts on the IT4I resources are for the exclusive use of the individual user named in the account application. Users are prohibited to share accounts with anyone.

All users are required to protect their private key against misuse or theft by encryption using strong passphrase of at least 8 characters. The passphrase must be kept secret, must not be stored unprotected in plain text, transmitted in plain text or made available to anyone.

All users are required to protect their system password. System passwords must be kept secret, must not be stored unprotected in plain text, transmitted in plain text or made available to anyone.

Users are prohibited from changing or circumventing access controls to allow themselves or others to perform actions outside their authorized privileges, as well as attempt to receive access information by unauthorized means.

Users must notify the IT4I immediately when they become aware that any of the accounts used to access the IT4I resources have been compromised.

IT4I personnel and users are required to address, safeguard against, and report misuse, abuse and criminal activities.

Users are prohibited from executing computationally intensive (intensive in terms of memory, cpu or I/O load) tasks outside the batch system.

Users may not deliberately interfere with other users accessing system resources.

Software use

All software used on IT4I computers must be appropriately acquired and used according to the appropriate software license agreement. Possession, use, or transmission of illegally obtained software is prohibited. Likewise, users shall not copy, store, or transfer copyrighted software, except as permitted by the owner of the copyright.

Users must not intentionally introduce or use malicious software such as computer viruses, Trojan horses, or worms.

Users are not allowed to reconstruct information or software for which they are not authorized. This includes but is not limited to any reverse engineering of copyrighted software or firmware present on IT4I computing resources.

Data use

Authors/generators/owners of information or data are responsible for its correct categorization as sensitive or non-sensitive. Owners of sensitive information are responsible for its secure handling, transmission, processing, storage, and disposal on the IT4I systems. IT4Innovations recommends use of encryption to protect the data from unauthorized access.

The IT4I systems provide protections to maintain the confidentiality, integrity, and availability of user data. Measures include the availability of file permissions, archival systems and parity and CRC checks on data paths and files, as well as other technical and organizational means. However, ultimately it is the user's responsibility to set access controls appropriately for the data.

In the event of system failure or malicious actions, the IT4I makes no guarantee against loss of data or that a user's data can be accessed, changed, or deleted by another individual. It is the user's responsibility to ensure the appropriate level of protection, backup and integrity checks on their critical data and programs.

Users are prohibited from taking unauthorized access to data or unauthorized actions to intentionally modify or delete information or programs.

User accounts, information and termination

Users should inform the IT4I promptly of any changes in their contact information (E-mail, affiliation, etc.) Updates should be sent to support@it4i.cz

Users may be attached to a Project upon request of Primary Investigator of that Project.

Users may be detached from a Project upon request of Primary Investigator of that Project.

Users who are not affiliated with IT4I and have not been attached to an active Project for more than 1 year will be deleted from the system and will need to reapply to regain access.

Responsibilities of Primary Investigator

The Primary Investigator (PI) is responsible for executing the Project, authorizing Users to participate on the project and utilization of the computational resources in order to achieve the Project's aims and objectives.

The PI agrees to provide reports detailing the Project's accomplishments. All Projects must complete a closeout report and other reports as requested.

The PI agrees to ensure that all publications or other outputs, that involved the use of IT4I resources contain the following credit line: This work was supported by The Ministry of Education, Youth and Sports from the Large Infrastructures for Research, Experimental Development and Innovations project „IT4Innovations National Supercomputing Center – LM2015070“. All such publications have to be registered at <https://extranet.it4i.cz/portal/feedbacks/publications>

The PI agrees to report to the IT4I when a project member leaves the Project.

Unlawful State aid

The PI as well as Users commit to adhere to regulations contained within the Communication from the Commission (of the European Union) “Framework for State aid for research and development and innovation” under No. 2014/C 198/01

<http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52014XC0627%2801%29>

(hereinafter as “Framework”), especially but not exclusively the article 2.2.2 of the Framework.

All parties acknowledge that the IT4I commits to adhere to the Framework and act in accordance with the Framework. Therefore, provision of computational resources on supercomputing must not constitute unlawful public financing or unlawful State aid.

User accountability

Users are accountable for their actions and may be held accountable to applicable administrative or legal sanctions.

Misuse of IT4I resources or noncompliance with the Acceptable Use Policy can lead to temporary or permanent disabling of accounts, loss of allocations, and administrative or legal actions.

Personal information agreement

The IT4Innovations retains the right to monitor all activities on its systems.

Users acknowledge that data regarding their activity on the IT4I systems will be collected. The data are collected for the purpose of understanding typical patterns of users’ behavior on the system in order to further improve the services provided by the IT4I. Another goal is to identify intrusions, misuse, security incidents or illegal actions in order to protect the IT4I systems and its users.

Users agree that this data may be processed to extract information contributing to above stated purposes.

No personal data will be disclosed to third parties.

Warranty disclaimer

Although designed as highly available, robust and secure, IT4I’s HPC systems are provided to our users without any warranty or commitment to a particular service level. IT4I accepts no responsibility for the performance of the codes and services, nor for the correctness or completeness of the outputs and results obtained.

Limitations to applicability

This policy may be subordinate to a contract or other higher level document governing relations between the user and the IT4Innovations. In case such a document exists, particular items of this policy may be void.