# Acceptable Use Policy of the multifunctional high performance computing complex "AVITOHOL" at IICT-BAS

## General Use Policy

### 1. Introduction

1.1. This Acceptable Use Policy (AUP) applies to all Users of the resources of the Multifunctional High Performance Computing Complex (MHPCC) "AVITOHOL".

1.2. For the purposes of this AUP, the following terms will have the following meanings:

1.2.1. *Resources* are all ICT facilities which are provided as part of the MHPCC "AVITOHOL" infrastructure;

1.2.2. The *Resource provider* is the body authorized to keep the Resources functional, usable and in good working order and to award access to the Resources;

1.2.3. The *User* means such individuals who have been approved to use the Resources;

1.2.4. *Malicious Software* means computer virus, Trojan, worm, logic bomb or other harmful material;

1.2.5. *Project* means the research work carried out by a group of users;

1.3. The purpose of this document is to define the rules and terms governing acceptable use of resources (core hours, license hours, data storage capacity as well as network connectivity and technical support), including access, utilization and security of the resources and data.

1.4. The Resource provider may make any reasonable changes to this AUP at any time and will inform the users. If the User does not accept these changes, it may cease to use the Resources at any time.

1.5. All users are requested to sign the Acceptable Use Policy (AUP) document.

1.6. The User shall follow also the acceptable use policies of the networks that he is using to access the Resources, e.g., the networks of BREN, IICT-BAS, BAS and the acceptable use policies of any other bodies or projects that mediated your access to the Resources.

### 2. General Use

2.1. The User will have regard to the principles which require that MHPCC "AVITOHOL" is used exclusively for peaceful purposes and conduct its activities in an ethical manner.

2.2. The User agrees that logged information, including information provided for registration purposes, is used for administrative, operational, accounting, monitoring and security purposes only. This information may be disclosed, via secured mechanisms, only for the same purposes and only as far as necessary to other organizations cooperating with the Resource Provider. Although efforts are made to maintain confidentiality, no guarantees are given.

2.3. The User will inform the Resource Provider if there are any changes to its contact information.

2.4. The User agrees to use the resources only to perform work, or transmit or store data consistent with the stated goals and policies and conditions of use as defined by the Resource Provider.

2.5. The right to use Resources is strictly personal and may not be transferred to any other third party. The Resource Provider are entitled to regulate, suspend or terminate the User access, within their domain of authority, and the User shall immediately comply with their instructions. The rights to use Resources will terminate when the period of allocation comes to an end.

2.6. The User recognises that the use of Resources by nationals of certain countries may be restricted by policies laid down by the the Resource Providers.

2.7. The User will respect all proprietary rights (which may also be considered intellectual property) belonging to the Resource Providers, including any copyright and licences.

2.8. The User will keep confidential all information which is obtained through the use of the Resources which it may reasonably be expected to know is confidential or sensitive.

2.9. The Resource Provider reserve the right to manage the usage of Resources in order to ensure full optimisation of the Resources, even if this may cause some limitation of usage for the User or changes to the Resources.

2.10. The User will not transport any data, which it may reasonably be expected to know is confidential or sensitive, e.g. credentials on IT equipment without adequate protection (such as encryption) in place.

2.11. The use of Resources is at the risk of the User. The Resource Provider don't make any guarantee as to their availability or their suitability for purpose.

2.12. Resource Provider will not be liable for any damages suffered by the User.

2.13. The User will exercise all reasonable care when accessing Resources.

## 3. Unacceptable Use

3.1. The User will not use Resources for any unacceptable purposes. Unacceptable purposes include but are not limited to:

3.1.1. any activity which is illegal under local, national or international law;

3.1.2. any attempt to breach or circumvent any administrative or security controls;

3.1.3. any creation, storage, use or transmission of data which is in breach of any copyright or licence;

3.1.4. any activity which purposely causes material or moral damage to the Resource Provider, or which causes loss of operational efficiency, or loss or corruption of Resources;

3.1.5. any activity which interferes with the use of Resources by other users;

3.1.6. any activity which compromises the privacy of other user;

3.1.7. any activity which may lead to the use or distribution of Malicious Software.

## 4. Security

4.1. It is the responsibility of the User to protect the details of its user account and access credentials.

4.2. The User will not divulge its access credentials.

4.3. The User will not use any other user's credentials to access the Resources.

4.4. The User will take all reasonable steps necessary to protect the security of personal computers, laptops and workstations, from which he accesses the Resources, against unauthorised access. Recommended security measures include the use of password-protected screensavers and locking and/or shutting down terminals when left unattended or not in use.

4.5. The User will not use any computer applications which jeopardise the functioning of Resources. The Resource provider will notify the User concerned who will be required to take all steps necessary to detect the cause and prevent reoccurrence. The Resource provider have the right to suspend the User's access to the Resources if necessary and to prohibit any computer application which, in its reasonable opinion, poses a security threat.

4.6. The User agrees to comply on use with any special conditions which may apply to specific software installed on the Resources.

4.7. The User will report immediately to the Resource Provider if it becomes aware of any unauthorised use of its user account, or if it knows or suspects that there has been a breach of security or misuse of the Resources. Failure to do so will enable the Resource Provider to terminate the User's use of Resources.

## 5. Liabilities and Sanctions

5.1. The User will be liable for any damages resulting from the infringement of this AUP or any other policies or conditions imposed by the Resource Provider and which have been communicated to the User.

5.2. Any infringement or potential infringement will be notified to the User in writing. If the infringement persists and/or further infringements are detected and/or where it is justified by the seriousness of the infringement, the Resource Provider may withdraw access rights to Resources and/or initiate disciplinary proceedings and/or legal proceedings against the User.

# Particular Use Policy

## 6. Access to MHPCC services

6.1. MHPCC services are provided on shared resources. To ensure equitable access for all projects certain restrictions on acceptable use are necessary. All use of MHPCC services must adhere to the following guidelines. Accounts repeatedly violating these guidelines will have their HPC access disabled.

6.2. Access to the HPC and GRID clusters is to be via ssh to respective login nodes or other interfaces that may be intended for direct access (eg Web Portals) and all access to compute nodes must be via LSF (Platform Load Sharing Facility). Direct access to compute nodes is not permitted.

6.2.1. A maximum number of concurrent login sessions will be enforced on login nodes;

6.2.2. ssh sessions that have been idle for an amount of time will be automatically disconnected;

6.2.3. These limits will be adjusted as necessary to manage login node resources and to comply with applicable security standards.

6.3. Processes that use significant compute or memory resources must not be run on any of the shared login nodes. These processes can be run via LSF or on a dedicated login

node. Processes running on shared login nodes that have used significant CPU time or that are using significant memory resources will be terminated without notice.

6.4. Scratch file systems are intended to be used as data storage for running jobs or under active analysis. Use of techniques for purpose of protecting files from the automated purge of scratch file systems is not permitted. Files on these file systems may be deleted at any time and are not backed up - the only copy of important files should not be kept on these file systems.

6.5. Users are expected to make efficient use of the resources to extent feasible jobs run on MHPCC.

6.6. Resources requested for jobs should be as accurate as possible even if such requests result in longer queue waiting times (eg if jobs require majority of per node memory they should use exclusive option even though this will likely increase the time the job will wait in queue).

6.7. Compute nodes which have lost contact with LSF for more than a few hours or which are unreachable from the console will be rebooted without notice.

6.8. The information regarding logging onto MHPCC resources, using LSF, specifying resource requirements, available storage options, etcetera is available on the appropriate “how to” pages.

## 7. MHPCC User access awarding

7.1. Every person, intending to become MHPCC User, have to fill and sign the following request forms downloaded from the MHPCC site:

7.1.1. Request form for MHPCC User access awarding

7.1.2. Request form for MHPCC User local account assignment

7.2. The Resource provider awards or denies User access to the Resources within period of 7 days via e-mail.

7.3. The period of MHPCC access for the particular User starts after the signing of two copies of this AUP from Resource provider authorized representative and the User.

Name and surname of the Resource provider authorized representative: _____

Signature of the Resource provider authorized representative: ----------

Date: _____

Name and surname of the User: _____

Signature of the User: ----------

Date: _____