

## **CINECA supercomputing facilities Access Policy**

### **Introduction:**

This Access Policy (AP) applies to all users of the CINECA supercomputing facilities. CINECA may make any reasonable change to this AP at any time. If the user does not accept these changes, it may cease to use the CINECA Supercomputing facilities at any time. User means the individual who has been authorised to access and use the CINECA HPC Resources. For the purposes of this AP, the following terms will have the defined meanings:

- CINECA System means the high performance computing facilities installed in CINECA;
- Resources means the high performance computing service made available by CINECA;
- Username means the identification name assigned to each individual User who has been authorised to access and use the Resources;
- Account means any right to have access to Resources as previously defined. The conditions under which an Account is activated may refer, but are not limited to, formal contracts, awards, tests and development, training and education. The Resources access is defined through a Project with an authorized budget;
- Period of Availability means the time period allocated by CINECA to the User for accessing and using the CINECA Resources;
- Malicious Software means computer virus, Trojan, worm, logic bomb or other material which is malicious or technologically harmful;
- Intellectual Property Rights (IPR) means:
  - a. Patents, inventions, designs, domain names, trade marks and related goodwill and trade names (whether registered or unregistered) and all rights to apply for registration of the same;
  - b. Copyright and related rights, database rights, know-how and confidential information;
  - c. All other intellectual property rights and similar or equivalent rights anywhere in the world which currently exist or are recognised in the future; and
  - d. All applications, extensions and renewals in relation to any such rights.
- GDPR means the General Data Protection Regulation that becomes enforceable on 25 May 2018 and aims at the protection of personal data for all individuals within the EU

### **General Use:**

- The User agrees to the enrolment, processing and transmission of the personal data asked for by CINECA;
- The User will inform CINECA of any changes to his/her personal enrolment information;
- The User will use the Resources only in conjunction with the purposes for which the Account is activated, the overriding objectives of CINECA and this AP;
- The User must inform CINECA in case his activity requires the loading and processing of data that may fall under the GDPR (personal data), in order to identify the appropriate security level; in any case the User confirms that sensitive or personal data will not be loaded and processed to CINECA resources without CINECA written authorisation;
- The Username is strictly personal and may not be transferred to any other third party. The rights to use the CINECA Resources will terminate when the Account is exhausted or expired;
- The User recognises that policies laid down by CINECA may restrict the access to CINECA Resources by citizens of certain countries;

- The User will respect all IPR belonging to CINECA, including any copyright and licence;
- The User agrees to not remove from the CINECA System any data without the explicit or implied permission of its owner;
- Use of the CINECA Resources is at the risk of the User. CINECA does not make any guarantee as to their availability or their suitability for purpose;
- CINECA excludes all liability for representations, statements, conditions or warranties to that or any other effect except to the extent that such liability may not be lawfully excluded;
- The User will exercise all reasonable care when accessing the CINECA Resources.
- The username will survive for a limited period after the end of all the related Accounts. The User will be allowed to manage and download the data in this period. One month before the expiration of the username, the User will be notified of the imminent expiration. After the expiration of the username, all data stored in the User's personal workspace will be deleted.
- The right to use CINECA Services ends when the original purpose is no longer valid or in specific circumstances the User has parted from the User's affiliated organization. In the latter case, the Principal Investigator (PI) of the Project decides whether the User can continue using Services even if affiliated to a new organization. If the User is the PI of the Project, the User must contact the party who has made the Project allocation to verify its eligibility. In any case, the PIs have the right to associate and remove third users (collaborators) from their account. The User Account and associated content will be handled according to the corresponding service descriptions and their terms of use.

#### **Unacceptable Use:**

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

- Any activity which is illegal under local, national or international law;
- Any attempt to breach or circumvent any administrative or security controls;
- Any creation, storage, use or transmission of data which is in breach of any copyright or licence;
- Any usage not allowed by the EU AI act (<https://artificialintelligenceact.eu/>);
- Any activity which causes material or moral damage to CINECA, or which causes loss of operational efficiency, or loss or corruption of the CINECA System;
- Any activity which interferes with the use of the CINECA Resources by other users;
- Any activity which compromises the privacy of other users.

#### **Security:**

- CINECA will provide the User with a username and a link to a portal where User can set the password and activate two-factors authentication (2FA) access. The link has a time validity. It is the responsibility of the User to protect the details of his/her username, password and 2FA token; The User will not divulge its credentials to any third parties, unless expressly authorised to do so by CINECA. The User will not use any other user's username to access the CINECA Resources;
- At login time, if needed, User will be requested to authenticate itself. Once the authentication has taken place, the server will issue a time-limited certificate needed by the User to connect to CINECA systems.

- Passwords should be changed as often as needed in order to guarantee a reasonable security to CINECA's system access;
- The User will take all steps necessary to protect the security of personal computers, laptops and workstations 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;
- The User will not knowingly introduce onto the CINECA System any Malicious Software and will not misuse the Internet in any way;
- The User will use the latest versions of anti-virus software available from an industry accepted anti-virus software vendor on all of its access systems to check for and prevent the introduction of Malicious Software onto the CINECA System;
- The User will act immediately to remove any Malicious Software from CINECA System. The User will not interfere with any anti-virus application software run by CINECA;
- Software that is required for the access of the CINECA Resources should be installed on the personal workstations in a protected partition or in a secure mode. That software will be maintained by the User and regularly updated for ensuring security updates;
- The User will not use any computer applications that jeopardise the functioning of the CINECA System. CINECA will notify the User, who will take all steps necessary to detect the cause and prevent re-occurrence. CINECA has the right to suspend the User's access to the CINECA System if necessary and to prohibit any computer application that, in its reasonable opinion, poses a security threat;
- CINECA will endeavour to protect the confidentiality of information stored on the CINECA System. Any information stored on the CINECA System will be used by CINECA, or any third party authorised by CINECA, for administrative, operational, monitoring and security purposes only;
- The User with administration privileges on IaaS cloud resources (VMs) will be responsible to maintaining the security (security patch, fix) on those resources. The User will also have the responsibility to backup both VMs and volume data.
- The User agrees to comply with any special conditions that may apply to specific software installed on the CINECA System;
- The User will report to CINECA if he/she becomes aware of any malfunction of the CINECA System or any problem in accessing the CINECA Resources.
- The User will report immediately to CINECA if he/she becomes aware of any unauthorised use of its username, or if he/she knows or suspects that there has been a breach of security or misuse of the CINECA Resources;
- The User must take suitable precautions to take care of his/her data once the Service comes to an end. Data are property of the User and are connected to the username;

#### **Liabilities and Sanctions:**

The User will be liable for any damages resulting from the infringement of this AP or any other policies or conditions imposed by CINECA with the exception of simple negligence. Any infringement or potential infringement will be notified by CINECA to the User in writing. If the infringement persists and/or further violations are detected and/or where the seriousness of the violation justifies it, CINECA may withdraw access rights to the CINECA System and/or initiate disciplinary proceedings and/or legal proceedings against the User. CINECA will not be held liable for any damage resulting from an interruption of the infrastructure

access service from which injury to users and possible third parties results.

**User Responsibilities:**

Each person making use of CINECA computing resources assumes certain responsibilities.

I have read the CINECA Access Policy and I understand my responsibilities as a CINECA User.

**Responsibilities Agreement \***

Not Agree

Agree