TGCC USER POLICY

cea

TGCC

Très Grand Centre de calcul du CEA

TGCC User Policy

The purpose of this document is to define the rules for the proper use of the services provided by TGCC.

This English version is for information only, the French original version shall prevail.

In the case of non-compliance with these rules, CEA reserves the right to ban access to the system to any user.

1 DEFINITIONS

- ✓ In this document, “TGCC” refers to the *Très Grand Centre de calcul du CEA*, and includes all the services made available to the users of TGCC.
- ✓ "TGCC services" refers to the hardware, software, applications, databases, networks and the digital files hosted at the TGCC computing centre.
- ✓ "Internet services" refers to any mean to exchange information (such as the internet, email, forum, telephony, videoconferencing, etc.) provided by local or remote servers.
- ✓ The term "user" refers to any individual accessing or using the TGCC’s services.

2 TERMS OF USE

- ✓ The use of these services must be reasonable in order to avoid saturation and must comply with the rules defined in the present User Policy.
- ✓ The services are only to be used for the purposes for which they were granted. This excludes, in particular, all personal use.
- ✓ Users may not use the services for illegal or immoral purposes. Moreover, the user shall abstain from any information exchange with sites harming CEA’s interests or image, such as sites related to pornography or online gambling, for example.
- ✓ Users may not use the resources for exchanging political, social or religious information and opinions.
- ✓ The user shall not infringe copyright or other intellectual property rights and not take data from any database or dataset without the explicit or implied permission of its owner.
- ✓ Users who create files which may be subject to the French Data Protection Act must take care of the procedures required by the *« Commission Nationale de l'Informatique et des Libertés »* (CNIL). They must also ensure that data processing complies with CNIL’s legal provisions. Moreover, the CNIL has also to be notified of the deletion of these files.

3 SECURITY RULES

- ✓ The user shall contribute to the overall security of the TGCC's services and comply with these security rules. In particular:
  - The user is responsible for his/her accounts and for any actions conducted with these accounts;
  - The user is responsible of the proper management of his/her authentication credentials. In particular, the password must be sufficiently protected, and not accessible in plain text – either digitally or physically;
  - The user shall protect his/her computer or workstation from any access by third parties (locking the workstation when absent, etc.);
  - The user shall rely only on the IT equipment made available to him by his company (or entity);
  - The user connects to TGCC only via the network of his/her company declared in the account creation form, or via a third-party site or services, that have been authorised by TGCC. Only the IP address declared in the account creation form will be accepted.
- ✓ The user ensures - at his/her level - the physical and virtual protection of the TGCC's services. To this end, he/she shall:
  - Not provide unauthorized user(s) access to TGCC services;
  - Not use or attempt to use accounts other than his/her own, nor attempt to mask his/her identity;
  - Ensure that the sensitivity level of the information he/she handles is compatible with the security rules of the site and recommendations mentioned above;
  - Not access information and documents stored on TGCC services other than his/her own, and those public or shared. He/she must not attempt to read, modify, copy or destroy public or shared files and folders;
  - Keep shared data to the minimum number of people who have to have access;
  - Protect sensitive information they hold by limiting access to this information to those who have to know;
  - Refrain from accessing any information held by a third party, in particular by capturing his/her password or by identity theft;
  - Inform the user service (hotline.tgcc@cea.fr) at the earliest of any indicated attempted breach of his/her account, and more generally of any anomaly he/she may observe.
- ✓ The user is – at his/her level – responsible of persevering the well-functioning of TGCC's services. To this end, he/she shall:
  - Not interfere with the proper functioning of TGCC's services, in particular by introducing non-professional data (documents, data, programs), malicious software or by circumventing security systems;

- Refrain from any improper use or any use likely to damage TGCC services, their configurations or their properties.

4 LOGGING AND TRACING

- ✓ CEA may implement controls regarding the general use of TGCC services by the users (including data spaces, hard drives, internet activities, and professional email) in order to identify possible breaches to this Policy.
- ✓ The control systems set up for the analysis of individual user activities (logging of connections or visited sites, volume and nature of files stored or exchanged, etc.) have been declared to CNIL, specifying their purpose, the data collected, the means of access to this information and their retention period.
- ✓ The personnel authorized to implement these control operations abides to reinforced confidentiality obligations. The authorised personnel may not divulge any information they may become aware of in the course of their duties, in particular information covered by the mail secret or concerning the user's privacy.
- ✓ In compliance with its legal provisions, CEA has set up a system for logging Internet access, professional e-mails and exchanged data.
- ✓ System administrators are responsible for ensuring the proper operation and security of TGCC's resources. As such, they have access to all information stored on or transmitted through TGCC services (e-mail, Internet connections, log files, etc.).
- ✓ CEA system administrators abide to reinforced confidentiality obligations. They may not divulge any information they may become aware of in the course of their duties, including information concerning mail secrecy or the privacy of users.

5 GDPR

- ✓ For the creation of the user accounts, CEA collects personal data with respect to GDPR. CEA declares being compliant with GDPR provisions (cf. Appendix 1 of the French Version for details on the GDPR procedures).
- ✓ Cloud Act
  - In case of a request by US authorities based on the Cloud Act for access to data processed by CEA, including personal data covered by RGPD rules, CEA will inform the user and his/her organization. CEA will also initiate, within a period of fourteen (14) calendar days, any form of legal action provided for by the Cloud Act or by any US law, in order to prevent, by any means the transmission of personal data.
  - Under no circumstances CEA will transmit any personal data without an enforceable decision by a French jurisdiction.