# CODE OF CONDUCT

# FOR THE USE OF CINES IT RESOURCES

## I. Introduction

### *A. Conditions for accessing CINES IT resources*

Access to the CINES IT resources is subject to acceptance by the user of this Code of Conduct.

An agreement giving full details of the projects and the conditions of use must have been signed by the CINES and the user's administrative manager.

### *B. Purpose of the Code of Conduct*

The purpose of this Code of Conduct is to define the regulations covering the use of the shared resources.

These regulations are based primarily on common sense and are intended solely to ensure that everyone can enjoy optimum use of the resources, taking into account the global constraints imposed by such shared use.

In the event of non-compliance with these regulations, the management of the CINES reserves the right to intervene to ensure that the greatest number of users are able to enjoy the most satisfactory working conditions possible.

The Code of Conduct also serves to inform users of current French legislation regarding computer fraud, as well as of the associated criminal penalties (separately from any administrative sanctions that may be applied by the relevant supervising body).

### *C. Computer crimes*

A number of recent laws have led to the emergence of an indisputable "right to the security of computer systems" (Article 323-1 Amended by Law 2004-575 of 21 June 2004 - Art. 45 JORF 22 June 2004, of the French Criminal Code – Illegal access to automated data processing systems):

> *"The act of fraudulently accessing or remaining in all or part of an automated data processing system is punishable by two years' imprisonment and a fine of 30,000 euros. If there is any deletion of or changes to any data contained in the system, or any alteration to the operation of that system, the penalty is three years' imprisonment and a fine of 45,000 euros."*

A complaint made by an establishment that has been a victim of an attempted fraud can therefore rapidly lead to serious criminal penalties.

## II. Definitions

### *A. Description of the resources*

The shared resources made available to users are the various UNIX servers running a wide variety of software (languages, databases, statistics, etc.), as well as the access network for these computers.

Connection through the RENATER network allows access to all or some of the services for communications with the Teaching and Research sector in France and abroad: email, file transfer, remote connection.

### *B. Area of application of the Code of Conduct*

This Code of Conduct applies to all local resources: servers, workstations, etc. as well as services accessible from the local computers (i.e. the whole Internet).

### *C. Suggested definition of parties involved*

#### 1. The User

A User is a consumer of the CINES IT resources.

This use must be associated with research, database activities or access to an email system / network.

#### 2. The Administrator

For each server there is one or more persons at the CINES who undertake the role of system administrators and who therefore have additional access rights.

## III. The rights and duties of Users

If there is a problem, users can request assistance from the Administrators to ensure that their rights are respected.

### *A. Individual information*

Each user must supply valid individual information: Address, project, etc. He/she must also notify the Administrator of any changes to this information.

The supply of deliberately misleading information will be deemed as being a serious offence resulting in a prohibition on accessing CINES IT resources.

### *B. Conditions of access*

Each user has a “userid” together with an associated password. The issuing of these two elements indicates a right of access, possibly restricted, to CINES resources for a given period. The resources to which the user has access can be limited on the basis of the user’s requirements and the limitations imposed by the sharing of these resources with other users.

This right of access to CINES resources is personal and non-transferable.
This right of access is temporary. It is withdrawn if the role of the user no longer justifies it.

It will be withdrawn if the user’s behaviour does not comply with the regulations as defined in this Code of Conduct.

Any means of access that may be provided for a user is also personal and non-transferable.

Each user is responsible for the use of the IT resources (local or remote) made through his/her account.

This means that certain basic precautions must be taken:

- The password must be at least 12 characters long,

- This password must be changed on regular basis,

- All sessions must be closed and workstations must not be vacated whilst a session is ongoing,

- The Administrators must be informed of any attempted security breach (even if unsuccessful) involving the account,

- Files must be protected (remove any unnecessary access),

- Digital supports must not be left unattended.

### *C. Respect for information of a confidential nature*

All personal files are private, even if they are physically accessible: The fact that a file can be read does not imply permission to do so.

Any attempt to read or copy files belonging to another user without his/her permission is therefore unacceptable. In addition, the interception of communications between users is subject to sanctions.

### *D. Respect for people*

Everyone has the right to work without being disturbed: freedom of speech does not imply any right to harass or insult others by means of a forum, email, or any other means of communication.

The fact that a file can be modified does not imply permission to modify it (any destruction or modification of user files is an act of vandalism).

Users must not take any action intended to limit or prohibit access to shared resources by other users.

The use of another person's identity is a criminal offence.

### *E. Respect for private resources*

Some of the resources (servers, printers, etc.) that are accessible through the network are not publically owned, whether belonging to specific users or whether they are special services that are not accessible to everyone.

Whilst physically protected resources are always private, those resources that are not physically protected may also be private: Users must determine whether this is the case before accessing these.

N.B.: Any unauthorised users can be disconnected without warning.

The use of private workstations and printers always requires prior authorisation. Some specialised servers may have access restrictions (e.g.: no interactive sessions on a file server).

Finally, some system files (that do not belong to any user) are readable for information purposes and these must never be modified, or even copied (most system files are covered by licenses). This obviously applies to all servers accessible through the network.

## IV. The rights and duties of Administrators

The CINES Administrators are responsible for the quality of the service. They must ensure that the rights and responsibilities of users are respected.

The CINES reserves the right to take any measures necessary to assume these responsibilities and enable the proper operation of the shared IT resources.

### *A. Availability of IT resources*

The CINES Administrators must inform users of any planned service interruptions.

They will work to minimise these interruptions and implement these at specified times and dates.

### *B. Respect for confidentiality*

CINES personnel must maintain the confidentiality of all user files, mails, and printed material to which they may have access.

### *C. Access to private data*

CINES personnel may have to access files or mails for the purposes of diagnosing or correcting problems. In ensuring that the system operates correctly or to verify the full application of the Code of Conduct they may be required to examine data that belongs to users. They are required to guarantee the confidentiality of any information to which they may have access in carrying out such tasks.

### *D Monitoring the use of the resources*

CINES personnel have the right to monitor the details of the working sessions of a user if there are any suspicions that the Code of Conduct is not being complied with.

They have the right to interrupt any user task in the event of an excessive use of resources that may be contrary to the optimum operation of the system (with or without notice, depending on the urgency involved in the incident).

They can move to an external support or compress any excessively large files or files that are not directly linked with “normal” work (with or without notice).

In the event of a deterioration in the service, they can terminate any work sessions that have been inactive for a period of time.

## V. Use of shared resources

The sharing of the resources of the CINES by a large number of users with a range of often very different needs implies compliance with a certain number of regulations.

### *A. Fair sharing of shared resources*

Disk space: The use of this must be monitored in order to keep any waste to a minimum (frequent cleaning, compression, archiving, etc.).

System: Processing that requires high resource use must make best use of off-line mode and off-peak hours.

Only the user level is authorised on a shared server. Unless agreed in writing by the CINES manager, such servers cannot be used for teaching system or network programing (developments relating to internal system functions, etc.). This prohibition exists in order to ensure the integrity of the system and the network.

The installation of “private” commercial software is allowed but the user must be able to provide evidence of a valid license if so requested by the CINES.

The installation of software or utilities that could damage the integrity of the systems is not allowed. This applies to any software that leads to an increase in the load on the computer, a malfunction, or a modification to the standard environment installed by the CINES.

### *B. Use of networks and systems*

The current level of interconnection between systems enables a high degree of user friendliness for the resources but does require strict regulations covering appropriate behaviour, breaches of which are subject to exclusion from the community.

The CINES resources must not be used for illegal connections to remote systems.

The following actions are deemed to be serious contraventions that can result in the immediate closing of that user’s account:

- Interruption of the normal operation of the network or of one of the connected systems,
- Access to the private information of any other user on the network,
- Modification/destruction of information on one of the connected systems,
- Actions that necessitate the use of additional human or technical resources to control what a user is doing on the network.

Furthermore, the development, installation or simple copying to one of the CINES servers of a program with the following properties is prohibited:

- Programs that allow other users to be harassed

- Programs for bypassing security
- Programs that overload the resources
- Virus and Trojan horse programs
- Programs that bypass software protection systems.

## VI. Compliance with legal restrictions on use

The IT resources of the CINES are intended for the uses as defined in the research agreements or dossiers. Some software may therefore be subject to restrictions on its use.

In addition, all current laws and decrees are fully applicable on all users.

### *A. Academic use of the resources*

No commercial uses are allowed unless authorised in advance by the CINES manager.

As some software is covered by special “educational” licenses, these must be checked before being used outside the research community.

### *B. Protection of software*

The same intellectual protection values apply for software and other academic publications (cf. Law of 3/7/1985).

For protected software: Copying is prohibited even for backup purposes (this will be carried out by the Administrators).

Illegal copying of software is theft.

Source code from protected software must not be included in any software that may be used externally.

### *C. Computer fraud*

The reference legislation is the French law of 5/1/88 (Godfrain Law).

The following activates are deemed to constitute offences:

- Fraudulent access or presence in a computer system,
- Deliberate attacks to disrupt the operation of a computer system,
- Attempts to commit these offences,
- Conspiracy or intention to commit these offences.

## VII. Possible penalties

Failure to comply with the regulations governing behaviour as defined in this Code of Conduct, as well as in the applicable laws, may result in administrative or criminal penalties.

### *A. Administrative penalties*

Any attempted intrusion by a user to another account, or the system, may result in the closing of all that user’s accounts on the resources of the CINES.

The CINES reserves the right to refuse access to any person having flouted this Code of Conduct.

Serious offences may be subject to administrative penalties in accordance with the penalties that are applicable within the supervising body.

### *B. Criminal penalties*

The CINES is legally required to report any infringements of the law. The CINES reserves the right to institute any criminal proceedings, independently of any other administrative penalty that may be enforced.

# CINES REGISTRATION FORM

I, the undersigned,

Identified on the servers of the CINES as user account (login):

User of the CINES resources in my capacity as:

Hereby certify that I have read and understood the “Code of Conduct for the use of CINES IT resources” and agree to comply with these regulations (the key elements of which are restated below).

Read and agreed

Montpellier, Date:

*Summary of some key regulations contained in the Code of Conduct for CINES users*

## Use of CINES IT resources

The CINES IT resources are specifically designed for scientific computing and databases.

The use of these by users from other backgrounds implies their compliance with certain essential regulations.

If these regulations are not complied with, the CINES management reserves the right to take action, in order to ensure that the largest number of users are able to enjoy satisfactory working conditions.

The Godfrain Law is intended to protect users against the “pirating” of their accounts or of the system itself.

## Guide to Correct Use

- CINES computers must only be used for authorised projects, excluding any other activity.
- Unless authorised by the CINES manager, CINES computers must not be used for the teaching of system or network programing purposes (developments making use of internal system functions, programing of "sockets"). In order to protect the integrity of the system and of the network only the user level is authorised for this type of teaching.
- Each user has its own individual login identification.
- Personal (name, first name, etc.) and administrative information enabling the identification of each user and his/her supervising body (laboratory, university, company, etc.) must be provided to the CINES system managers.
- Each user is responsible for his/her login identity. Specifically, he/she must make sure that the password used is sufficiently secure (it must not be found in a French dictionary nor consist of a simple juxtaposition between such a word and one or two numbers). It must have at least twelve alphanumeric characters.
- The sharing of a login between several users is not allowed. If any hacking occurs or in the event of any damage, the person holding that login will be held responsible.
- Any attempt using another login identification to access a system or computers outside the CINES over the CINES network will result in the immediate closing of the accounts of that user on the CINES computers.
- No software that could compromise the operation of the computers must be installed. This applies to any software that results in an additional load for the computer, a malfunction or any modification.
- The CINES is liable and sole webmaster for the “cines.fr” domain.