

INRIA Computer Network Policy on Access and Usage

This document sets out INRIA's policy on computer facility and network access and usage. This policy should be upheld by all users, at each of the Institute's Research Units, in the course of their usual activities. It does not cover activities specific to system and network administration.

1 Authorization of access to computer resources

1. Only properly authorized persons may access INRIA facilities. In most cases this authorization is provided in the form of an account issued in the name of the authorized person.
2. A user may not permit any other person, including other authorized users, to access INRIA facilities through his or her account.
3. This authorization is valid only for activities complying with current legislation and with INRIA's undertakings.
4. INRIA reserves the right to withdraw this authorization at any time and without previous notice.

2 Security

Each user is responsible for any and all activity initiated in or on INRIA facilities by his or her account. Each user is therefore responsible for security

at an individual level, with the help of the recommendations provided by the system administrators. In particular :

1. Each user is responsible for selecting a secure password, in line with the recommendations of the system administrators, and for keeping that password secret at all times. Passwords should never be disclosed to another person, including INRIA staff members.
2. Users are responsible for protecting their own files and data, and for any access rights that they issue to other users.
3. Users may not use accounts for which they have not received authorization. They must not attempt to use or crack another user's password.
4. Users may not intentionally develop or use programs that affect the operation and integrity of INRIA systems.
5. INRIA facilities and network connections may not be modified without authorization from site administrators, whether these connections are to internal or external networks.
6. Any violation, or attempted violation of the INRIA computer facilities should be reported to the system administrators and one of the staff members on the site responsible for security.
7. Users should follow the recommendations and instructions given by system administrators.

3 Intellectual property rights

Software may only be used in accordance with the law of July 3, 19985 on intellectual and artistic property rights, the recommendations of the copyright holders and the undertakings entered into by INRIA (in licence contracts, for example). In particular :

1. It is generally illegal to copy software, other than to make a back-up copy.
2. No commercial software may be installed on an INRIA site without checking with the head of computer resources that such an installation is authorized.

4 Connections and access to other sites

INRIA's facilities and networks allow users to dialogue with other computer sites throughout the world. Access to these sites may only be made in accordance with the regulations imposed by the site concerned, and in compliance with current legislation such as law 92-685 of July 22, 1992 on computer fraud. In particular :

1. It is forbidden to connect or attempt to connect to another computer system or computer network without the consent of the owner of the computer system or computer network.
2. Users may not intentionally use INRIA facilities for actions that may jeopardize the security or normal functioning of other computer systems or telecommunications networks.

5 Computer files and the rights of the individual

The law 92-684 of July 2, 1992 protects the individual against improper use of information about him/her contained in any computer file. In particular, it states that :

1. Any file containing the name of, and information about any individual may only be created once certain formalities imposed by the Commission Nationale de l'Informatique et des Libertés have been completed. At INRIA these formalities are carried out by the SAJAS (Service des Affaires Juridiques et Administration du Siège), which should be contacted, either directly or through the administrators of the site concerned, before any such file is created.
2. Any person whose name is contained in a computer file must be informed of the existence of the file, its purpose, the right to access the information contained therein, and how to do so at the time the information is obtained.

6 Confidentiality of information

1. Users must not attempt to read, copy, disclose or modify the files of another user without authorization.
2. Users must not attempt to intercept communications or messages between other users.
3. Users must not attempt to interfere with any information on the internal running of INRIA resources that may be obtained through the use of the computer facilities.
4. Users must take, if necessary with the help of those responsible for on-site security, data protection measures to respect the undertakings of confidentiality entered into by INRIA with its partners.

7 Proper use of facilities

1. Each user is responsible for ensuring that all facilities are used in an efficient, ethical and lawful manner. In particular, users must not monopolize shared resources, make excessive use of computational power, disk space, telecommunications networks, etc.
2. Users must behave in a responsible way in e.mail exchanges, discussion forums, newsgroups, etc. In particular, they should specify whether their contributions are made on a personal basis or on behalf of INRIA.