LABORATOIRE
DE L'ACCÉLÉRATEUR
LINÉAIRE

CHARTER ON THE PROPER USE OF THE ORSAY *LABORATOIRE DE L'ACCÉLÉRATEUR LINÉAIRE*'s INFORMATION SYSTEM RESOURCES

Introduction.

The information systems and hardware of the *Laboratoire de l'Accélérateur Linéaire*, UMR 6423, made available to personnel, are dedicated to research, teaching and administration. Most of this hardware is connected to a local network and through it to the Internet. Any user of this hardware thus belongs to a vast community which implies on his/her part the respect for certain safety and good behavior rules. Imprudence, negligence or malicious intent by a user can have serious consequences for the community.

This charter lays out the rights and obligations of each person and represents a mutual commitment between the user and all the laboratory's personnel. It is presumed to be known by all and is an integral part of the *Laboratoire de l'Accélérateur Linéaire*'s company rules.

The Different Players.

From an information system point of view, a distinction must be made between three categories of players:

- the users: all the people using the information systems made available to them
- the system and/or network administrators and IS security correspondents, technically responsible for the operation of the IS tools,
- the functional managers: Laboratory management, group or unit managers, teachers supervising the students for activities calling on IS resources.

Each category has rights and obligations which are identical in spirit but different in their application.

The Rights of All.

Each person has a right to:

- information relating to the common resources and services offered by the Laboratory and the IN2P3,
- information allowing that person to best use the resources made available to them,
- information on the security of the system being used.

The Obligations of Each Person.

- Each person has the obligation to respect the security rules applicable to the system being used; these rules consist of this charter illustrated by regularly updated appendices, as well as possible specific rules in connection with a particular work environment; these rules are available to each user via the functional manager or system administrator.
- Each person must respect intellectual and commercial property rights in compliance with current legislation.
- Each person must agree to refrain from obtaining knowledge of information belonging to others without their approval, from communicating to any third party such information or any non-public information to which that person may have had access but for which that person does not hold proprietary rights.
- Each person must clearly identify him/herself, no one may use another person's identity or act anonymously. Each person must notify any intrusion attempt on their account.
- No person may assign their rights to another. Access authorizations to IS resources are strictly personal and may not be assigned, either temporarily or definitively, to any person whatsoever (associate, friends, family members included) whatever trust may be held by that person.
- Each person must try to achieve their goal using the least costly means in terms of common resources (disk space, printouts, workstation occupancy, remote server occupancy etc.).
- Each person must contribute to improving the operation and the security of the IS tools in compliance with security rules and advice and by immediately notifying the managers of any observed anomaly, by sensitizing associates to the problems of which that person has knowledge. The installation of software which can jeopardize the security of IS resources is prohibited.
- Each person must limit their use of the hardware made available to them to strictly professional use and comply with the functions assigned to them which excludes use for personal or commercial purposes.
- No person can change any equipment either in terms of hardware or system software nor connect a machine to the local network without the express approval of the system and/or network administrator.
- No loss or indemnity may be claimed pursuant to the alteration, destruction or loss of confidentiality of the processing of non-professional information by the system administrators in the fulfillment of their professional functions if such processing was implemented on a Laboratory IS resource by a user at his/her own risk .
- No person can connect equipment which is not the property of the Laboratory on the local network without the approval of the system administrators who have the authority to require the means to administer it without restriction. This charter shall apply to said equipment and its owner shall become a user thereof under this charter.

Specific Rights and Obligations of System and/or Network Administrator.

The administrator technically has extensive powers over many systems. As a result the administrator's obligations are important, in particular that of not abusing of his/her powers. The system administrator is responsible for the security of the machine and/or the network under his/her care. The IS security correspondent belongs implicitly to this category.

Any System Administrator has the right to:

- be informed of the legal implications of his/her work, in particular as regards the risks run should a user of the system under his/her responsibility commit an objectionable action,
- access, on the systems he/she administers, private information for system diagnostics and administration purposes, scrupulously respecting the confidentiality of this information refraining unless otherwise required from altering them,
- establish surveillance procedures for all the tasks performed on the machine to detect breaches or attempted breaches of this charter, under the authority of his/her functional superior and in association with the IS security correspondent,
- take conservatory measures if required by an emergency without prejudice to sanctions resulting from breaches to this charter which are the responsibility of the functional managers.

Any System Administrator has the obligation to:

- inform the users on the extent of his/her technical powers pursuant to his/her position,
- inform the users of and sensitize them to information security problems inherent to the system, to inform them of the security rules to be followed, assisted in this by the IS security correspondent,
- follow the general network access rules defined for the local network, and beyond that IN2P3, Renater and the Internet in general,
- follow confidentiality rules by limiting access to confidential information to what is strictly necessary and by respecting professional secrecy in this regard,
- follow, if he/she is a user of the system, the rules required by him/her of other users,
- configure and administer the system with a view to improved security in the interest of the users,
- inform the IS security manager of IN2P3 of the implementation of exceptional surveillance or investigation procedures,
- immediately inform his/her functional superior and the IN2P3 IS security manager of any intrusion attempt (successful or failed) on his/her system or of any dangerous user behavior,
- cooperate with the security correspondents of the outside networks in the event of a security incident involving a machine administered by him/her.

Specific Rights and Obligations of the Functional Managers.

The functional managers of information systems have the right to:

- temporarily or definitively prohibit access to information resources by a user who fails to comply with this charter,

- refer serious faults resulting from the failure to comply with this charter to the superiors which may lead to disciplinary or criminal procedures.

The functional managers of information systems have the obligation to:

- inform all the players of, disseminate this charter by any appropriate means,
- appoint an IS security correspondent,
- communicate the name of the system administrators of all the machines placed under their authority to the Laboratory IS security correspondent,
- support the system administrators and IS security correspondent with their authority in their work in applying this charter.

Sanctions Incurred in the event of Non-compliance.

Failure to comply with the rules laid out in this charter may lead to two types of sanctions:

- disciplinary sanctions:

  - the functional managers have full authority to take the necessary conservatory measures in the event of non-compliance with this charter and to prohibit the defaulting users from accessing the IS resources and the network,

  - these defaulting users may be referred to the competent disciplinary committee,

- civil and/or criminal sanctions:

  The evolution of electronic techniques and information technology has led the legislator to define sanctions in keeping with the risks to individual liberties and law arising from the uncontrolled use of IS files and processing.

This charter, an integral part of the company rules of the *Laboratoire de l'accélérateur linéaire*, has been communicated to all the Laboratory's personnel and applies to each member of that personnel.

Adopted by the Council of the *Laboratoire de l'accélérateur linéaire*, 28 November 1998,

The Director of the *Laboratoire de l'accélérateur linéaire*