Charter for the use of ESRF Computing Resources (translation of the original French Charter)

Annex to the Internal Regulations - implementation 19/12/2005

1. Introduction

The present charter defines the rules for the use of ESRF computing facilities. It cancels and replaces all previous notes concerning the use of computing facilities.

The charter should be communicated to all Users of ESRF computing facilities, whether internal or external. It is also part of the official documents given to external people upon arrival on the ESRF site. It shall be posted on the official notice boards and can be consulted on the ESRF Intranet. Finally this charter is included in the **Internal Regulations ("Règlement Intérieur")** kept at the disposition of every employee.

2. Definitions

For the purpose of this charter :

- The term **"ESRF computing facilities"** includes:
  - All PCs (Personal Computers including those which are self-service), laptop computers, workstations, servers and peripheral systems (such as printers), directly or indirectly connected to any ESRF computing and/or telecommunication network;
  - All support utilities, program libraries, applications, as well as all documentation, electronic mail, Intranet and Internet services installed or running on any of the computers and making use of the above-mentioned networks.
- The term **"Users"** refers to any person making use of ESRF computing facilities.
- The term **"Management"** refers to Directors and Heads of Divisions.
- The term "**System/network Administrator**" refers to any ESRF employee specifically responsible for the operation and security of the ESRF computing facilities and appointed individually and in writing.

3. Basic principles

ESRF computing facilities shall be used in accordance with ESRF's objectives and as part of the Users professional duties. Nevertheless, the personal use of the ESRF computing facilities is tolerated as specified in chapter 4.

The ESRF endeavours to maintain and protect its computing facilities. It cannot, however, guarantee their proper functioning or perfect confidentiality of the information stored.

4. Personal use of the ESRF computing facilities

The personal use of ESRF computing facilities is tolerated, provided that:

- it is in compliance with the present charter,
- it is not detrimental to official duties, including those of other Users,
- the frequency and duration are limited and there is a negligible use of ESRF resources,
- it does not constitute a political and/or commercial profit-making activity,
- it does not violate applicable laws.

In case of conflict on the application of these standards, the Director General will have the final decision.

5. Rights of the Users

Each User has the right to be informed about the proper use of the computing equipment, which has been allocated to them. The User will also dispose of information about the inherent safety and security of computer tools. Additional information and recommendations are available on the Intranet. If need be, the system and/or network Administrator can be consulted.

6. Duties of all Users

Users have the following duties, every time the ESRF computing facilities are used:

- **Regarding ESRF interests:**
  - Should the User have access via computing facilities to confidential information, they must respect such confidentiality.
  - Users must respect the integrity and confidentiality of data belonging to the ESRF.
  - Computing resources must not be used to undermine the image of the ESRF.
- **Regarding the security of the ESRF systems and networks:**
  - It is forbidden to voluntarily perturb the ESRF computing facilities.
  - Users must respect the technical and security advice supplied by the system and/or network Administrators or by Management (e.g. protection against viruses).
  - It is forbidden to seek unauthorised access to accounts, which are forbidden to the user in question.
  - It is forbidden to look for, disclose or exploit any security weakness in the ESRF network and/or computing facilities.
- **Regarding security of ESRF Users:**
  - Users shall ensure, as far as possible that their Personal Computers or workstations are protected against unauthorised access. They shall also protect their personal account by avoiding obvious passwords and by changing their passwords regularly. If necessary, the system and/or network Administrator may advise them.
  - It is forbidden to disclose their passwords to any third party, unless absolutely necessary to carry out the activity of the company. If the User is absent, he/she must be informed upon return that the PC has been used.
  - Upon request from a system and/or network Administrator, Users shall select a new password.
  - It is forbidden to use a third party account and password, or to act in an anonymous manner.
  - Users shall respect the privacy of other Users' information. It is forbidden to modify, falsify, distribute information belonging to another User.
- **Regarding the use of computing resources:**
  - Users shall respect the intellectual and commercial proprietary rights related to the ESRF computing facilities, (including software copyrights). In particular, all Users must be in possession of the appropriate licence for all software used. All software developed at the ESRF remains the property of the ESRF (see note on Intellectual Property).
  - Users shall use ESRF computing resources in a way that will not impede the work of other Users or their access to the network. If such a work is likely to overload the network, Users must ask the system and/or network Administrators for prior approval.
  - Users who have been given an account with privileged access in connection with specific professional duties, they shall advise their direct supervisor and the system and/or network Administrator as soon as those duties no longer require privileged access.
  - It is mandatory for the User to return all ESRF computing equipment when he leaves the ESRF (end of the contract) and in return he/she will be allowed to recover personal information by his/her means.

- **Regarding the use of the Internet:**
  - It is illegal to use ESRF resources to load, consult, stock, publish or distribute documents or information liable to undermine the respect of the human being and his dignity. In particular, this concerns documents of pedophile, revisionist or racist nature, or documents that undermine the integrity of the individual by violating the secret of correspondence, threat, insults, harassment, etc.
  - This also applies for usages that attack property, especially fraud and offences under the Code of Intellectual Property.
  - Personal web-pages are authorised only if they are linked to the professional activity (CV, scientific publications). A dedicated section of the ESRF web server is available for this purpose.
- **Regarding the use of E-mail:**
  - Unauthorized access to, forgery and diverting of e-mail is strictly forbidden.
  - Spamming is forbidden i.e. – emails sent in large quantities: to more than 20 addresses, unless it is for professional or for unions' use *(see agreement concerning the use of intranet by the trade unions on 06.10.05)* **,** chain messages (messages received individually in the context of collective dispatches asking to forward them collectively) and wide distribution of advertising messages inside and outside the ESRF.

7. Rights of system and/or network Administrators

The system and network Administrators may only exploit, upon their own initiative, or upon orders from the supervisor, the information to which they have access in order to secure the good functioning and the security of the applications.
The ESRF system and/or network Administrators in charge of normal functioning and security of the network and systems are allowed to have access to information in ESRF computing facilities in order to:

- Solve problems affecting ESRF computing facilities, such as viruses etc; perform upgrades and to install new equipment.
- Detect computer security weaknesses or computer security violations or attempts to violate the computer security.
- Monitor available resources to ensure the adequacy of ESRF computing facilities.
- Investigate, upon written orders from the Director General, in case of a suspected infringement of this present charter by a user.
- Remove accounts when a User's contract with ESRF is terminated.

On a regular basis, system and/or network Administrators use the following tools to monitor the e-mail and Internet traffics:

- Storage of the Web links consulted (registering the computer connected, the site name, the date, and the size of the file consulted);
- Daily compilation of Web statistics (the top ten ESRF computers using the Web and the top ten Web sites visited);
- Storage of e-mail exchanges: time, size, sender, destination, (not the contents nor subject on the message server).

8. Duties of system and/or network Administrators

- System and/or network Administrators have the obligation to inform Management of computer security problems they detect on the ESRF network.
- Any personal information susceptible to be acquired by the system and/or network Administrator using the above-mentioned tools (chapter 7), must be dealt with in confidence.
- The Administrators are relieved of their obligations of confidentiality in two cases:
  - Upon written request from the Director General, in the case where correct functioning of the systems and/or the interests of the ESRF are questioned (1).
  - Application of legal and regulatory provisions compelling the Administrators to disclose information.

(1) *For example, the application of this written request by the Director General is applied in case of malfunctioning of the network and which may be put down to misuse by employees such as : surfing on forbidden sites, taking part in spamming operations, opening of a personal internet site on the ESRF installation etc…*

9. Rights of Management

According to French law ("Informatique et Libertés" 6 January 1978, n° 78-17), Management, after having been informed in particular by the system/network Administrator, may in case of serious indications :

- Have the Administrator carry out a control of the computing equipment in the presence of the suspected employee or of a staff representative if the employee is absent.
- Deposit a formal request at the competent court for authorisation to have computer traces or data seized.

The system/network Administrator must inform Management of the existence of serious indications, which are liable to justify such measures, but at the same time he must respect his obligation of confidentiality in particular concerning the contents of the information he may have acquired.

10. Duties of Management

Management must make sure this charter is distributed, applied and respected in the various Divisions. In this framework the group leaders must also participate.

11. Sanctions

The non respect of the present charter may lead to :

- Suspension or suppression of the access to the computer facilities,
- Disciplinary sanctions: according to chapter 3 of the Internal Regulations ("*Règlement Intérieur"),*
- Civil liability or criminal responsibility, according to the law, **including the non-respect of confidentiality rules set out in chapter 8**.

Reminder of some useful references for the comprehension of this charter:

Law n° 78-17 of 06/01/78 Informatique et liberté, law n° 2004-801 of 06/08/04 cf. **http://www.cnil.fr**
Legislation relative to computer fraud (article 323-1 to 323-7 of the penal code), **(cf. www.legifrance.gouv.fr/citoyen/code.ow,** puis « Code pénal », « chapitre III : des atteintes aux systèmes de traitement automatisé de données »).
Legislation relative to intellectual propriety
(cf. www.legifrance.gouv.fr/citoyen/code.ow, puis « Code de la propriété intellectuelle »).

I, the undersigned……declare that I am fully aware of the regulations regarding my contract.

The Employee
(I agree)