CHARTER FOR THE USE OF ESRF COMPUTING RESOURCES

(Translation of the original French Charter)

Annex to the Internal Regulations - Implementation 19/12/2005 – Revision 04/05/2015

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 applies 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.

The revision dated 04/05/2015 adds an appendix titled "COMPUTING CHARTER FOR THE USAGE OF OWNCLOUD AT ESRF".

2. Definitions

For the purpose of this charter:

- The term **"ESRF computing facilities"** includes:
  - All ESRF desktop or laptop computers (including those which are self-service), workstations, servers, other computing equipment like tablets, and peripheral systems (such as printers), directly or indirectly connected to any ESRF computing and/or telecommunication network.
  - The computing network including wireless techniques (Wi-Fi).
  - 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 reasonable and there is a negligible use of ESRF resources,
- it does not constitute a political and/or private 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/network Administrators can be consulted.
Users can store personal data in clearly identified folders, named "Personnel" or "Personal" or "Perso" or "Private" or "Privé", with any character being either upper-case or lower-case.

with any character being either upper-case or lower-case.

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/Network Administrators or by Management (e.g. protection against viruses).
  - It is forbidden to seek unauthorised access to accounts.
  - It is forbidden to look for, disclose or exploit any security weakness in the ESRF computing facilities.
- **Regarding security of ESRF Users:**
  - Users shall ensure, as far as possible that their ESRF computers are protected against unauthorised access.
  - Users shall ensure that their ESRF computers are locked when left unattended.
  - A System/Network Administrator may force users to change their password.
  - 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.
  - 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 licences 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 ESRF computing facilities. If such a work is likely to overload the ESRF computing facilities, users must ask the System/Network Administrators for prior approval.
  - Users who have been given an account with privileged access in connection with specific professional duties shall advise their direct supervisor and the System/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/she 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, store, 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 forbidden.
  - Spamming is forbidden i.e. – emails sent in large quantities: to more than 50 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.
  - Important recommendations:

- Users must always pay attention to the URL of a website that is included in a received e-mail, even when the e-mail comes from people they know. Only an URL corresponding to an official internal ESRF Web site must be followed (ex. http://intranet.esrf.fr).
- Users must not submit personal or financial information in Web forms that do not belong to an official internal ESRF Web site; if this has to be done, Users must do their best for checking the reliability of the Web site.
- Users must not reveal personal or financial information in e-mails they send, and must not respond to e-mail solicitations for such information.
- Users must be extremely cautious when opening e-mail attachments, even when the email comes from people they know. If an e-mail or e-mail attachment seems suspicious, users must not open it, even if the anti-virus software indicates that the message is clean.

7. Rights of System/Network Administrators

The System/Network Administrators may only exploit, upon their own initiative, or upon orders from their supervisor, the information to which they have access in order to secure the good functioning and the security of the applications.
The ESRF System/Network Administrators in charge of the normal functioning and security of the ESRF computing facilities are allowed to have access to any information 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/Network Administrators use the following tools to monitor the e-mail and Internet traffic:

- Storage of the Web links consulted (registering the computer connected, the site name, the date, and the name and 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);
- Daily compilation of network statistics (the top ten users on wireless networks, the top hundred users on the EPN Campus of the Internet link, etc.);
- Storage of e-mail exchanges: time, size, sender, destination (not the contents nor subject of the e-mail).

8. Duties of System/Network Administrators

- **System/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/Network Administrator using the above-mentioned tools (chapter 7), must be dealt with in confidence.
- The System/network 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 System/network 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 ESRF computing facilities 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 System/network 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.**

APPENDIX: COMPUTING CHARTER FOR THE USAGE OF OWNCLOUD AT ESRF

Date of application: as soon as OWNCLOUD is operational at ESRF

This charter complements the ESRF Computing charter, which is part of the Internal Regulations ("Règlement Intérieur"). The use of ownCloud must conform to both the ESRF Computing charter and the specific rules given in this document. The non-respect of the rules may lead to the enforcement of sanctions mentioned in the Computing charter.

1. Introduction – What is OWNCLOUD?

OWNCLOUD is a software system for what is commonly termed "file hosting". As such, OWNCLOUD is very similar to the widely used Dropbox (or Microsoft's Windows Azure or Apple's iCloud or Google's Cloud platform) with the primary difference being that ownCloud is free and open-source and data does not reside on servers belonging to an external company. ESRF is operating ownCloud on its internal servers to the benefit of ESRF staff members and/or in view of collaborations with other research laboratories.

ownCloud's main features:

- Simple and universal access via a Web interface
- File sharing under your control
- File versioning – for keeping old versions of a file
- File synchronization – a file modified on one computer can be automatically updated on the other computers, provided a client program is installed on the participating computers.

Data stored on ownCloud is accessible from internal ESRF computers, but also from private computers or devices like smart-phones, be they located on ESRF premises or outside the ESRF – at home, on mission, etc.

2. Definitions of terms

For the purpose of this charter:

- The term "ownCloud" refers to the central disk storage system that provides the ownCloud service.
- The term "User" refers to any person making use of ownCloud at ESRF.
- The term "ESRF device" refers to computing equipment provided and supported by ESRF, be it located in ESRF premises or elsewhere.
- The term "External device" refers to computing equipment not provided by ESRF.

3. Basic principles

ownCloud shall be used in accordance with ESRF's objectives and as part of the Users' professional duties. The ESRF endeavours to maintain and protect its computing facilities. It cannot, however, guarantee their proper functioning nor perfect confidentiality of the information stored.

4. Usage of ownCloud

4.1. Limits

Data Storage on ownCloud must adhere to the following rules.

- Must be used in compliance with the present charter and with the ESRF Computing Charter.
- Unlike the other computing tools where personal use is tolerated within certain limits, ownCloud shall be used for professional purposes only. It must be noted that all files stored on ownCloud are accessible by System Administrators, who are subject to the rules defined in the ESRF Computing charter.
- Shall not be used for political and/or private commercial profit-making activity.
- Does not violate applicable laws, including copyrights.

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

4.2. Additional duties of Users - relevant abstracts of the Computing Charter

- Users shall respect the intellectual and commercial proprietary rights related to the ESRF computing facilities (including software copyrights).
- It is illegal to use ESRF resources to load, consult, store, publish or distribute documents or information liable to undermine the respect of the human being and his/her 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, threats, insults, harassment, etc.
- This also applies to usages that attack property, especially fraud and offenses under the Code of Intellectual Property.

4.3. Data confidentiality

Users must not use ownCloud for sharing sensitive data with external individuals:

- personal data related to staff members – for instance remuneration elements,
- commercial and/or financial data - like the status of a Call For Tender, or the budget for a project,
- data undermining the image of the ESRF.

5. Support provided to Users by TID/SC (Systems and Communications group)

Any use of ownCloud with the latest release of Firefox and Internet explorer is supported, but not Web browsers on External devices, nor Web browsers other than Firefox and Internet explorer on ESRF devices.

When the ownCloud client program is used for synchronising data between devices:

- support is provided only for ESRF devices located on ESRF premises,
- no support is provided for ESRF devices located outside ESRF premises, the device must be brought back at ESRF to be supported,
- no support is provided for External devices, even when located on ESRF premises.

Users are invited to pay attention to the backup of important data files. It must be noted that ownCloud integrates a feature for recovering deleted files, but this feature may be useless in case of a major disaster.

6. Storage space provided to Users

Requests for storage space larger than the default must be addressed to TID/SC and will be examined before approval.

==========

Some useful references for further information and comprehension

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)