Direction des Systèmes d'information, des infrastructures et des services (DSI)

CHARTER FOR USE OF COMPUTING RESOURCES

17 May 2011

Auteur(s) : Gérald Masini, Bertrand Wallrich

Version : 1.4 **Date :** 17 mai 2011

Référence : charte-inria_1.5_EN.doc **Pages :** 10

Diffusion : INRIA

Suivi des versions

Version	Date	Objet
1.5	28/03/2011	Corrections de la version 1.4 de l'ancienne charte en anglais- francais

SUMMARY

1. Preamble

As INRIA is a *Public Science and Technology Research Centre* (EPST), it has to preserve and protect its scientific and technological patrimony[1] (renown, information system, data...) according to current laws and regulations.

This charter is aimed at making this possible. It defines the rules for using computing and telephony resources in observance of the law, in order to protect the interests of the Institute and to to establish users' confidence regarding the fears of interference with privacy posed by new technologies.

The charter supplements the INRIA internal regulations about the working and use of INRIA computing resources. It was approved at the joint technical committee meeting of 2 July 2007.

2. Definitions

The specific terms used throughout this document are defined as follows:

- **Computing resources**
  Any equipment (workstation, PDA, computing server, management server, storage server, printing server, wired and wireless local networks, mobile or landline telephones, etc.) made available to INRIA users and either locally or remotely accessible.
  Users must also comply with this charter when working with **personal equipment.**
- **Data**
  Any information stored on an INRIA computing resource, whatever its kind (email, text file, image file, sound file, etc.) and scope (professional or personal) are.
- **Management of INRIA**
  Under the Managing Director of INRIA, management of computing resources is delegated to the INRIA research unit heads and to the central and center's IT Service managers.
- **Privileged user**
  A user with technical privileges (administrator rights) that he can used to bypass the data protection systems of a computing equipment.
- **Public**
  A set of individuals having access to a piece of information.
- **Chief Security Officer (CSO)**
  A system administrator in charge of the security of the INRIA information system (CSO[2]), or a security correspondent in an INRIA research unit (CSOC[3]).
- **Systems administrator**
  An individual working at INRIA within an IT Service, in charge of the administration of shared computing resources, to ensure their correct working, availability and reliability.
- **User**
  Any person working at INRIA on a permanent or temporary basis (regardless of his/her employer), including external personnel either invited to or hosted by INRIA and students granted with access authorisation. Further, the notion of user extends to any person collaborating with INRIA and having an INRIA IT account opened within the context of the collaboration. Further, any person who has not an IT account (a visitor) is considered to be a member of the public, even if he/she has access to few resources (e.g. Wi-Fi network access).

[1] INRIA is classified ERR (Establishment under Restrictive Regulation), and is submitted to a regulation that requires high-level protection of scientific and technological data.
[2] chief security officer.
[3] chief security officer correspondent.

3. Scope of application

This document sets out the rules for correct use of INRIA computing resources, rules that any user must conform to either when working in any INRIA site or when using mobile equipment for professional purposes (laptop, mobile phone, etc.).

Violation of any of these rules can lead to internal disciplinary actions and, in ncase of violation of legislation or regulatory, to prosecution being taken. The various laws relevant to this document are supposed known, in particular:

- Law 78-17 of 6 January 1978, amended, about data processing, data files and individual liberties,
- Law 88-19 of 5 January 1988, amended, known as *Loi Godfrain*, about computer fraud,
- Law 92-597 of 1 January 1992, amended, in *Code de la Propriété Intellectuelle*,
- Law 2004-575 of 21 July 2004, amended, known as *LCEN: Loi pour la Confiance dans l'Economie Numérique*.

4. Acces rights to computing resources

The use of INRIA computing and phones resources is subject to prior authorisation, validated by INRIA Management or its relevant delegates: department manager, or research project manager, system administrator, etc. This authorisation is affirmed by the opening of an IT account.

Unauthorised use of computing resources is tantamount to intrusion into the INRIA information system and, as such, will be considered as an offence (Article 321-1, para. 1, of the Penal Code). This includes a visitor accessing resources other than those made available to the public by INRIA.

This authorisation is strictly personal and must in no way be transferred, even temporarily, to a third party.

This authorisation only applies to activities that comply with the missions of INRIA and of its partners, and with current legislation.

This authorisation applies to any IT resource used within the context of professional activity (including Association Delegations).

Professional activity is such as set out by INRIA, i.e. research, technical development, technology transfer, dissemination of scientific, technical and cultural information, experimentation of innovative techniques, training, as well as any administrative and management activity implied by or associated with such activities.

In case of violation of these rules, the Management of INRIA reserves the right to withdraw this authorisation at any time and without notice.

5. Professional and private use

Private use of computing resources is tolerated as long as it remains within reasonable limits, is not detrimental to professional activity, complies with current legislation, has no commercial or profitable end (online sales, advertising, etc.), and does not interfere with the renown of INRIA.

Private or personal data must be clearly tagged as such, and it is the user's responsibility to do so[4]. Data not tagged as such are considered to be professional data.

The user must remove all personal data when leaving INRIA, prior to having his/her IT account closed. Any remaining data are considered to be professional data.

6. Data protection and confidentiality

We all have a duty to protect data from loss, theft, or modification. The Management of INRIA cannot be solely responsible for protecting data. Users must estimate the confidentiality level of their professional data and use appropriate protection measures, as recommended by the Institute:

- All users are responsible for the access permissions they knowingly set to their data (files), and must set permissions as appropriate to the desired confidentiality level;
- All users may protect their data using encryption solutions, and, in this case, do have the duty to provide the Management of INRIA with means of accessing the encrypted professional data;
- All users must avoid hosting any INRIA data with third parties but, if this becomes necessary, data may only be hosted with the security manager agreement;
- When data are submitted to specific confidentiality clauses, users must implement such solutions as advocated by the corresponding contract.

7. Security rules

All users are responsible for the use that they make of INRIA computing resources when using accounts created for them, or equipment made available to them. As such, users must make their individual contribution to security, in accordance with the recommendations of the CSO and CSOC.

Of particular note:

- All users must use secure access means (passwords, certificates, etc.) recommended by CSO and CSOC. These access means must be kept secret and in no way be communicated to any other party;
- All users must only use accounts for which they have been granted authorisation, to the exclusion of any other; they must not attempt to acquire or decipher another user's password;
- Users must not read, copy, disclose or modify another user's data without the prior authorisation of that user;
- Users must not intercept communications between third parties;
- All users must respect the means by which equipment is connected to local and external communications networks of an INRIA Research Center, such as set by the Management of INRIA; These connections may only be modified with the prior authorisation of the Management of INRIA;
- Any actual violation, violation attempt, or suspected violation of an information system must be reported to the CSO or CSOC;
- All users have the duty to adhere to recommendations defined by CSO and CSOC with regard to the use of computing resources and the security of their computing equipment;

[4]e.g. by placing personal data in a folder named *private* or *personal*, or by stating *personal* in the subject line of an email considered as private.

- Any user needing to depart from these recommandations within the context of his/her professional activity may only do so with the CSO and CSOC agreement.

8. Intellectual property

8.1. Copyright

The dissemination of a work or of its copy, either in whole or in part, to the public without the prior authorisation of the author(s) is prohibited. Software, databases, and other creations such as articles, images, web pages, music or video files, etc. are works according to the intellectual property code.

The copy or reproduction of a work is also prohibited, even when the work has been published by its author(s), regardless of the right to make a private copy or backup (which implies the obligation to posess a copy of the work acquired legally), and of rights applying to free software. This prohibition can be overridden by authorisation of the author(s) or of the editor(s)/producer(s).

The use of software (source or binary) and more generally of any document (file, image, sound, etc.) in a way that does not comply with the intellectual property code may constitute forgery.

The use of a software is usually subject to acquiring a license. Any software copy must be made in strict conformity with the commitments made by INRIA in the license agreement.

8.2. Personality rights

Pursuant to article 226-1 of the Penal Code, users agree:

- not publish information on the internet affecting the privacy of third parties,
- not publish images without the prior authorisation of the persons concerned,
- not build or publish recordings (voice, video, etc.) without the prior authorisation of the persons concerned.

8.3. Publication on the internet

The management of INRIA is bound by its responsibility in its capacity as editor and hoster ([5]), with regard to the data published on the sites for which it is responsible, and it can be held legally accountable in the event of circulation of illicit content. For this reason, users must not publish documents containing the following elements:

The management of INRIA is bound by its responsibility as editor and hoster, regarding data published on the sites for which it is responsible. It can be held legally responsible in case of dissemination of illicit content. Therefore, users must not publish documents containing the following elements:

- **commercial products or services:** any commercial practice and any advertising is prohibited in public teaching establishments, according to the status of EPST and of INRIA in particular;
- **libel:** in pursuance of Article 29 of Law 1881-07-29 of 29 July 1881 (amended), about offenses against the person;
- **racial hatred, negationism and revisionism:** in pursuance of Article 24 b of Law 1881-07-29 of 29 July 1881 (amended), about offenses against the person.

[5]Law 2004-575 of 21 July 2004, amended, (known as *LCEN*), for confidence in digital economy.

More precisely, a user may publish data related to his research activity or to his professional activity (curriculum vitae, non-confidential PhD thesis, bibliography, reference to achievements[6]), as well as explicit links to pages or websites external to INRIA websites (site related to research activity, personal website, etc.) in conformance with the legal context described in this charter.

In order to ensure correct application of these rules, the Management of INRIA may at any time inspect the content of published documents and take measures (document deletion, for example) in case of non-conformance with this charter.

9. Connections to websites

Internet use and access to websites must be in compliance with the rules specific to the various networks and websites used, and with the current legislation.

Of particular note:

- All users must conform to the charters of the networks they use, more particularly RENATER, which is the main access provider of INRIA;
- Navigation to websites must be established in conformance to their charters;
- Make massive copies of websites (with non-interactive download files tools) is prohibited without explicit agreement of the website owners;
- When using systems belonging to INRIA, when connected to INRIA networks, performing knowingly actions which endanger the security or the working of websites or of telecommunication networks is prohibited.

10. Electronic communication

INRIA computing resources provide various means of electronic communication (email, discussion forums, web-accessible documents, etc.). Such means must be used in accordance with the following rules:

- All users must show the highest degree of courtesy when communicating, regardless of the means used;
- All users speak in the name of INRIA within his executive function. They are invited to use a personal email address for all personal mailings;
- All users must ensure that the content of their communications complies with current legislation;
- All users must avoid impairing INRIA image or interests within their communications.

11. System administrators and privileged users

Systems administrators have the obligation to ensure the working and security of networks and computing resources. They are allowed to take any appropriate measure to assume their responsibilities, whilst observing professional ethics and discretion. In this respect, they may:

- use tools related to the specific nature of their activity, such as monitoring tools or computer hacking tools,

[6]Having taken care to validate the publication of this information with the industrial promotion departments.

- implement measurement systems for the purpose of system and network diagnosis or administration,
- take measures to deal with an operational or security incident; in this respect, they are allowed to retrieve all useful information, including by examining log files (connections, remote access, etc.); systems administrators then have the obligation of confidentiality. No other exploitation of these files or data shall be carried out on personal initiative, or under the authority of line management.

System administrators are required to absolute discretion. Except on requisition of the judiciary authority, they do not respond to any other requests for information or processing that may incriminate people or infringe their privacy.

Similarly, privileged users must not disclose any information that they are able to access using their increased permissions, and notably when such information is covered by secrecy of correspondence (article 226-15 of the penal code) or concerns users' private lives. Bound by professional secrecy, neither would they be obliged to do so, except by special legal provision.

Similarly, privileged users must not disclose information they could access thanks to their privileges, especially when the information is protected by correspondence secrecy (Article 226-15 of the Penal Code), or when the information users' privacy. Bound to secrecy, they also can not be compelled to do so, unless specific legislation to that effect.

Similarly, privileged users must not disclose information which they could access thanks to their privileges, especially when such information is covered by correspondence secrecy (Article 226-15 of the Penal Code) or is related to users' privacy. Privileged users are bound by professional secrecy: they cannot be compelled to do so, unless specific legislation to that effect.

12. *Commission Nationale de l'Informatique et des Libertés* (CNIL)

12.1. Declaration of nominative files

Law 78-17 of 6 January 1978, amended *(Loi Informatique et Libertés*), protects individuals against any abusive or malicious use of information about their person and contained in any kind of computing file.

Of particular note, the law provides that:

- The creation of any file containing nominative information must be subject to formalities with CNIL[7], before its implementation; These measures must be taken together with the CNIL correspondent (if designated), the CSO, and the Management of INRIA;
- Any person about whom information is recorded in a file must be informed of the existence of this file, of its purpose, of the existence of an access permission and of the modalities of its implementation, as soon as the information is collected.

A list of the CNIL declarations of INRIA is available on the INRIA website.

12.2. Managing logs

Systems Administrators use certain investigative means in order to fulfil their mission. Connection logs, electronic communications logs, Internet access logs, and data access logs concerning nominative files are declared to CNIL and are used in accordance with legislation.

These logs cannot be submitted to any automated processing, excepting an authorised access by Systems Administrators within the context of their work (security, search for a dysfunction, etc.). They

[7] *Commission Nationale de l'Informatique et des Libertés* : An independent administrative authority protecting privacy and personal data.

cannot be used for any other purpose, except with the prior agreement of the individuals concerned, or by justice decision.

Appendix: Recap of applicable legislation

Applicable legislation is part of Penal Code and of Intellectual Property Code, mainly:

- Law 78-17 of 6 January 1978, amended, on data processing, data files and individual liberties,
- Law 88-19 of 5 January 1988, amended, (*Loi Godfrain*) on computing fraud,
- Law 92-597 of 1 July 1992, amended, (*Loi sur la propriété intellectuelle*),
- Law 2004-575 of 21 July 2004, amended, (LCEN: *Loi pour la Confiance dans l'Economie Numérique*),

and, for information:

- Law 92-685 of 22 July 1992, reforming the Penal Code provisions about prevention of crimes and offences against persons,
- Law about "violations of the rules about cryptology" of 29 December 1990, amended 26 July 1996,
- Law 94-548 of 1 July 1994 (*Journal Officiel* of 2 July 1994) about the processing of nominative data for research purposes in the domain of health, amending Law 78-17 of 6 January 1978 about data processing, data files and individual liberties,
- Law 2006-64 of 23 July 2006, about fight against terrorism, including various provisions about security and border control,
- Article 226-15 of the Penal Code about violation of correspondence secrecy.