CHARTER FOR USING THE COMPUTER RESOURCES OF CENTRALE NANTES (ECN)

1 Preamble

The computer resources of Centrale Nantes (hereinafter ECN) are all connected via a local network, which is in turn connected to the OMEGA metropolitan network and the RENATER network (national network for technology, teaching and research), giving access to the Internet. Users of these resources are therefore part of a vast community, which means that they must respect certain security and good conduct rules.

In light of this, the purpose of this charter and the ECN internal rules is to:

- define rules for using ECN computer resources and those to which it allows access,
- specify the framework for using the network from student residences,
- build users' awareness of computer security issues,
- inform them about applicable laws and regulations.

This charter applies to every user of ECN computer resources, whether locally connected or using other remote connection solutions, which permit access to internal or external communication or electronic processing services via the ECN computer network, including access to services available on the internet. Each user must agree to respect this charter before any use of these resources.

This text can be subject to modification to include regulatory developments. The modification(s) will be notified to users by internal e-mail and documents referring will be updated accordingly.

2 Access to computer resources

All ECN permanent, temporary, hosted staff, staff of incubated companies and students are allowed to use ECN computer resources. However, each user must first accept the terms of this charter by signing it.

Prior authorization is then required to use the computer resources. This authorization usually takes the form of a request from an authorized person to open an account. Similarly, prior authorization is required from the competent persons in charge of running of these resources before connecting any equipment to the system.

These authorizations are strictly personal and may not under any circumstances be transferred to another person, even temporarily. These authorizations may be withdrawn at any time in case of violation of this charter or regulations in force.

Users shall lose their authorization to use ECN computer resources once they cease being a staff member or part of the ECN community. They must therefore notify the competent departments of any change resulting in any such loss of authorization.

3 Use of computer resources

The use of computer resources and internet services, along with the network to access them, is only authorized in the exclusive context of activities complying with ECN goals and applicable law.

These shared resources must be used reasonably and fairly. Each user must therefore make reasonable use of these resources. Users must also follow any recommendations given to them.

ECN may not be held liable for any damage, loss of data or information or breach of confidentiality resulting directly or indirectly from the use of its computer resources.

4 Rules of use, security and good usage

Each user is responsible for any personal use of the computer resources and networks to which they have access. Every user is also responsible for contributing to overall security at a personal level. In particular:

- passwords are the sole and unique control on access to the assigned computer resources. It is therefore very important to choose the right password. Passwords must be difficult for others to guess while easy to remember for users. See the following website: http://www.ssi.gouv.fr/particulier/bonnes-pratiques/ for a list of recommendations to follow. Logins and passwords must be kept secret and under no circumstances given to anyone, including ECN personnel . Keep in mind that never school services request them by any means whatsoever.
- each user must only use the accounts for which they have authorization. Hence, a user must always remain clearly identifiable when using the computer resources. In particular, when using internet services, users must only use the user name officially assigned to them.
- it is forbidden for any user to give unauthorized users access to the systems or networks via the user's computer.
- users must make no attempt to acquire or decipher another user's password or mask their real identity.
- users are not allowed to try and read, modify, copy or destroy any data other than their own, whether directly or indirectly.
- each user must ensure the physical safety of the equipment provided.
- users must never leave a personal or shared workstation with resources or services still accessible.
- users must also protect their own information and data by means of personal back-ups or the back-up solutions provided, or via a centralized collective solution.
- each user must follow the instructions specified by the Computer Resource Centre (hereinafter CRI) when connecting hardware to the internal and external communication networks. The CRI alone is authorized to supply the IP addresses of the hardware to be connected to the network. Connections may only be modified with its prior authorization. These instructions cover both hardware (physical connection) and software (system connection) aspects.
- any observed, attempted or suspected breach of a computer system must be reported to one of the system administrators for the group of machines concerned and to the CRI. As a general rule, the same is true for any anomaly noticed. In all cases, send an e-mail message to the following address: rssi@ec-nantes.fr (rssi = *Responsables de la Sécurité du Système d'Information or IT Security Managers*).
- each user has a duty not to damage the resources used. Any problem must be reported to the CRI as quickly as possible, so that corrective action may be taken rapidly.
- each user must follow the system administrator's instructions. In particular, anyone authorized to connect a specific machine onto the network agrees to acquire the necessary degree of competence to run it correctly and keep it at a satisfactory level of security, at least equal to that of the IT system as a whole.
- in particular, all users must comply with the systems established by the institution to fight against viruses or corruptions and attacks by computer programs.
- any user must not install, download or use, on any system of the institution, any piece of software whose licenses fees has not be fully paid, or not coming from reputable sites, or without advice of his hierarchy.
- in particular, the use ok skype software is prohibited.
- urban, regional and national networks must be used in line with the various charters that ECN has agreed to respect and have others respect. The content of the RENATER charter is available on this website: https://www.renater.fr/chartes.
- Internet services must be used in compliance with standard good conduct rules, known as Netiquette, which can be consulted at the following website: www.afa-France.com/netiquette.html

5 Obligation relating to intellectual property

Any software programme (source or binary) and, more generally, document (file, image, sound, etc.) must be used in compliance with the law on intellectual property, the copyright holders' recommendations and any undertakings made by ECN (in licence agreements, for example). In particular:

- it is strictly forbidden to make copies of commercial software programmes for any use whatsoever, other than a back-up copy made under the conditions stipulated by the intellectual property code.
- a software programme may only be installed in compliance with applicable law, the copyright holder and publisher's instructions and CRI recommendations. It may be subject to payment of a licence fee.
- it is forbidden to override any restrictions on a software programme's use.

6 Obligations relating to the security and integrity of computer systems and data

ECN facilities allow users to log on or dialogue with websites all over the world via the RENATER network. The user therefore acknowledges being apprised of the security rules relating to the use of the RENATER network described on this website: https://www.renater.fr/chartes and undertakes to respect the obligations therein.

Furthermore, other websites must be accessed in compliance with the specific rules of usage of the websites and networks and according to the legislation in force, such as the law on computer fraud. In particular:

- it is forbidden to log on or attempt to log on to another website without the site administrators' permission.
- it is forbidden to use systems connected to ECN networks to engage in any actions that might endanger the security or functioning of the ECN computer system or other websites and telecommunications networks, whether deliberately or by carelessness. It is therefore forbidden to install, use and develop any programmes that might have that effect.

Users also agree not to cause – directly or indirectly – any disruption in the functioning of the network and computer systems they access, nor to cause any modification, alteration or destruction of data or files other than those of which they are the author.

7 Confidentiality obligation

- each user may only access publicly available data or files on the network and their personal data or files. It is forbidden for users to try and acquire data or files reserved for other users, even if these elements are not protected by hardware or software devices. Any infringement of this obligation may result in civil or criminal prosecution of the offender.
- any attempt to intercept communications between other users is forbidden.
- each user is bound by a duty of non disclosure concerning any information about the internal functioning of ECN acquired by using these computer resources.
- each user must also take the necessary data security measures, with the system administrators' help if need be, to comply with the confidentiality commitments ECN has made to other parties.

8 Analysis and control of use of resources

For legal reasons and security, maintenance and technical control requirements, the use of hardware and software resources and exchanges via the network are recorded in files. These files are saved and then archived for the legal period authorized and may be used when required to identify the origin of a malfunction or a user's misuse or malice.
Any such action must be done in compliance with the applicable law, particularly the law n° 78-17 of 6 January 1978 on computers, files and freedoms.

9 Rules of good usage in electronic communications

ECN computer facilities permit the use of many electronic communication aids (e-mail, discussion forums, file downloads, etc.). These communication aids must be used with great care, in accordance with the applicable law and the following rules:

- each user must specify whether they are making a personal statement or speaking on behalf of ECN, particularly in any message for public circulation.
- each user must refrain from harming ECN's image or interests in their communications.

10 Special case of clubs, associations and other

In the specific context of the use of computer resources by clubs, associations and students in residences, ECN has a special status as network service provider. The applicable legal framework is therefore that of the law n° 2000-719 of 1st August 2000, amending law n° 86-1067 of 30 September 1986 on freedom of communication which limits or even exempts ECN from liability. In this special context, ECN is bound by an obligation to exercise vigilance and due care with regard to any offences committed, but is not in any way bound by a performance obligation.

Consequently, ECN must take every step to avoid the access to illicit content via its computers. This applies to the web pages of clubs and students' associations hosted on CRI servers, for example. Similarly, action will be taken to rapidly put an end to any illicit behaviour by anyone using computers logged on from a students' residence.

The user is nonetheless liable in all cases. ECN may ask a bailiff to record the offence, file a complaint against the offender and/or take private legal action for compensation, in order to protect itself from lawsuits or legal complications.

11 Reminder or principal texts and laws

Please note that everyone in France must respect all applicable legislation, particularly in matters of computer security:

- the law on data privacy (*Informatique et liberté*)
- the legislation on intellectual property
- the law on the confidentiality of correspondence sent by means of telecommunications
- the legislation on computer fraud (particularly articles 323-1 to 323-7 of the Criminal Code)
- the law on the use of the French language
- the law on press offences, notably punishing libel, revisionist ideas, racism and abusive language
- the legislation on broadcasting and telecommunication with regard to key principles applying to public and private communications
- the applicable legislation on encryption
- the legislation on free speech
- the legislation for trust in the digital economy
- the legislation on communicating to the public by electronic means
- the legislation covering personal data processing security

All these texts are constantly updated and may be consulted on the CNIL website and that of LEGIFRANCE, which publishes most French laws free-of-charge. The website addresses are: http://www.cnil.fr/ and http://www.legifrance.gouv.fr/

12 Sanctions

Failure to respect any of these rules may lead to internal disciplinary measures by ECN. Furthermore, any user breaking the law may be prosecuted.

I, the undersigned, declare that I have read this "Charter for using the computer resources of Centrale Nantes" and I agree to follow the rules herein. I am aware that if I infringe these rules, Centrale Nantes may cancel my access to its facilities, without prejudice to any legal proceedings that may be brought against me.

First and Last name : _____

Laboratory / Department : _____

Date : _____/_____/_____

Signature : _____

P.S : Please sign this page, then:

- for undergraduate and master's students, send it back to the administration department
- for doctorate students, permanent, temporary, hosted staff and staff of incubated companies, send it back to the CRI.