Computer Charter for University of Nancy 2

Approved by the Administrative council July 10, 2001

The current charter has the objective of defining the rules of use of the data processing resources at the center of University of Nancy2, in particular to precise the responsibilities of users. Following this will permit normal and optimal use of the data processing resources as well as the internet service in use by the establishment.

1. Applicable domain of charter

The rules and obligations set forth by this charter apply to all persons, in particular professors, researchers; faculty-researchers, student; administrative and technical staff, whom are authorized to use the data-processing resources and systems of University of Nancy2.

The former is comprised; specifically, of the servers, administrative work stations and micro-computers, computer equipped classrooms, and University laboratories and documentation centres

Respect of the rules defined by the current charter are likewise extend to use of the system by those outside the university; system access through an intermediary of the established school network, for example, the internet network.

2. Conditions for Access to the data processing network of the university

The normal use of the data processing systems of the School has the sole purpose of undertaking activities of research, teaching, or administration. Without the prior permission of the university utilization of realization of projects not relevant to the missions of the university or missions trusted in the user are not permitted to. Each user may use the access codes according to his needs (access Internet, Intranet, with the business applications, particular servers, etc). The access codes given are personal and inalienable. The user of the codes is responsible for the use for which it is made. The password should correspond to a word or proper name in any language. Each user commits to not communicating this password to a third party.

The user will warn the persons in charge of data-processing if an access code no longer enables connection, or if he suspects that an account was broken into. Generally he will inform the data-processing person in charge for any anomaly which he may note.

3) Compliance with the rules of the data-processing deontology :

Each user, is legally responsible for the use that they make of the data-processing resources, commits himself to comply with the rules of the data-processing code of ethics, particularly in not intentionally carrying out operations which could have consequences such as:

- Masking ones true identity;
- Use of the password of another user;
- Deterioration, or modification of data or reaching of information belonging to other users without their authorization;
- Attack of the integrity or sensitivity of another user, in particular via messages or provocative images;
- Halt or disruption of the normal operation of the network or one of the systems connected to the network;
- Modification or destruction information on one of the systems;
- Connection or attempt at connection on sites without being authorized.

The creation of a program having objectives such as the aforementioned is also prohibited. If in the achievement of his work or missions, the user is brought to constitute files, under the data-processing law “and freedoms” imposed, under this constitution, the files comprising a processing of personal data must have a declaration of objective or a request for opinion in front of the Data-processing National Commission and Freedoms (CNIL).

La réalisation d’un programme informatique ayant de tels objectifs est également interdite. Si dans l’accomplissement de son travail ou des ses missions, l’utilisateur est amené à constituer des fichiers, il est rappelé qui la loi « informatique et libertés » impose, préalablement à leur constitution, que les fichiers comportant un traitement de données nominatives fassent l’objet d’une déclaration ou d’une demande d’avis après de la Commission Nationale Informatique et Libertés (CNIL).

4) Use of software:

The user may use software only after the advice of the qualified data processing department. The user will in no case:

- Install software without authorization and in particular games;
- Make a copy of a commercial software;
- Circumvent the restrictions of a software;
- Develop programs constituting as or being connected with viruses.

5)Use of data-processing resources

Each user must take care of the data-processing material and premises laid at their disposition. They will inform the IT service of any anomalies which may occur. The user must do their best to not occupy the entirety of their disk space and should make optimal use of modes of compression available for their files. Use of the resources must be loyal and rational so to avoid saturation of files.
All computers which belong to a department, laboratory, or service must be connected to the network through a computer specialist of the university. The former ensures the rules of security are well respected.

A user may never leave work open without proper disconnection.

6)Specifics at the disposition of student users

Management of student email boxes
All the students of the University of Nancy 2 have a personal email. The size of this is limited. To avoid dysfunctions of the service, the data processing department may remove the oldest messages if the email box reaches its capacity. More generally, modifications of the parameters of transport may be made to ensure operation.

7) Information for users under the management of the data-processing systems and resources

Responsibilities of the administrators of the system/network SGDB
The administrators of the system/network SGDB are the persons who oversee the machines which are connected to the University network as well as the servers which install the different services at the disposition of users(internet network, management applications, educational services, research and documentation services).

- The administrators are in charge of ensuring the quality of the service provided to users with in their limited allotted means. They have the right to proceed with all steps necessary to ensure the good functioning of the means of data-processing of the university.
- The administrators are held with the task of informing the users, with any possible measure, of all necessary interventions that are likely to disturb or interrupt the normal use of the resources.
- The administrators are held with the task of immediately informing those in charge of security of all possible intrusions into the system or of any unlawful behaviour of a user.
- It is imperative the administrators respect the privacy of a user’s files

Files of Tracing
All services used yield, at the time of their use, “the files of tracing”. These files are essential for the administration of the systems. They in effect remedy any dysfunction of the system or services used. These files contain such information as those concerning the email (date, destination, etc.) as well as the hours of connection to management applications, to the network from a distance, the number of machines used for the services, etc…
These files of tracing exist for the entirety of internet services. These files are not to be used save for a technical usage. Always, within the framework of judicial procedure, the files are at the disposition of the president or judicial review, upon the president’s accord.

Viruses
Tools are put in place for the protection against viruses.

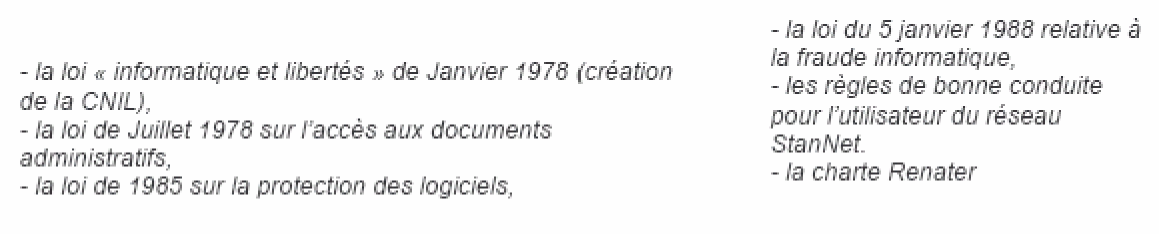
- The antivirus software on each uses account have the capacity of the following strategy: If a virus is detected, the software will attempt to repair the file, if the attempt fails the file will be destroyed.

- The email service is also equipped with an antivirus software as they may receive viruses emitted from outside the Nancy2 systems. Both the sender and receiver(s) will be notified if a virus is detected and the message subsequently not sent.
- Other software may be put in place to protect the university system and data of the users.

The user who disobeys the rules defined above exposes themselves to the loss of their data-processing account, as well as disciplinary proceedings

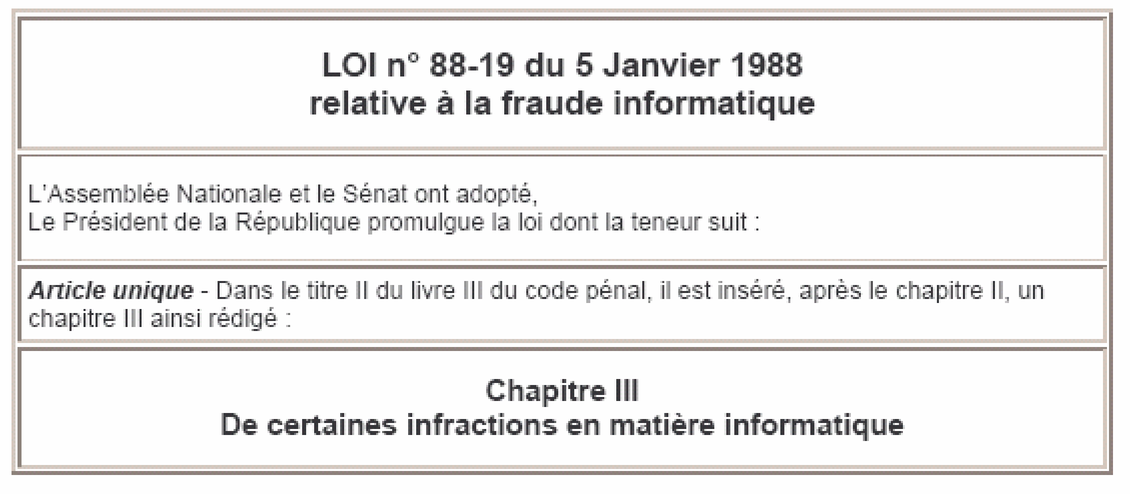
Penalties, defined by the effective legislative and regulatory texts.

For reference to other texts, they are as follows:



- la loi « informatique et libertés » de Janvier 1978 (création de la CNIL),
- la loi de Juillet 1978 sur l'accès aux documents administratifs,
- la loi de 1985 sur la protection des logiciels,

- la loi du 5 janvier 1988 relative à la fraude informatique,
- les règles de bonne conduite pour l'utilisateur du réseau StanNet.
- la charte Renater

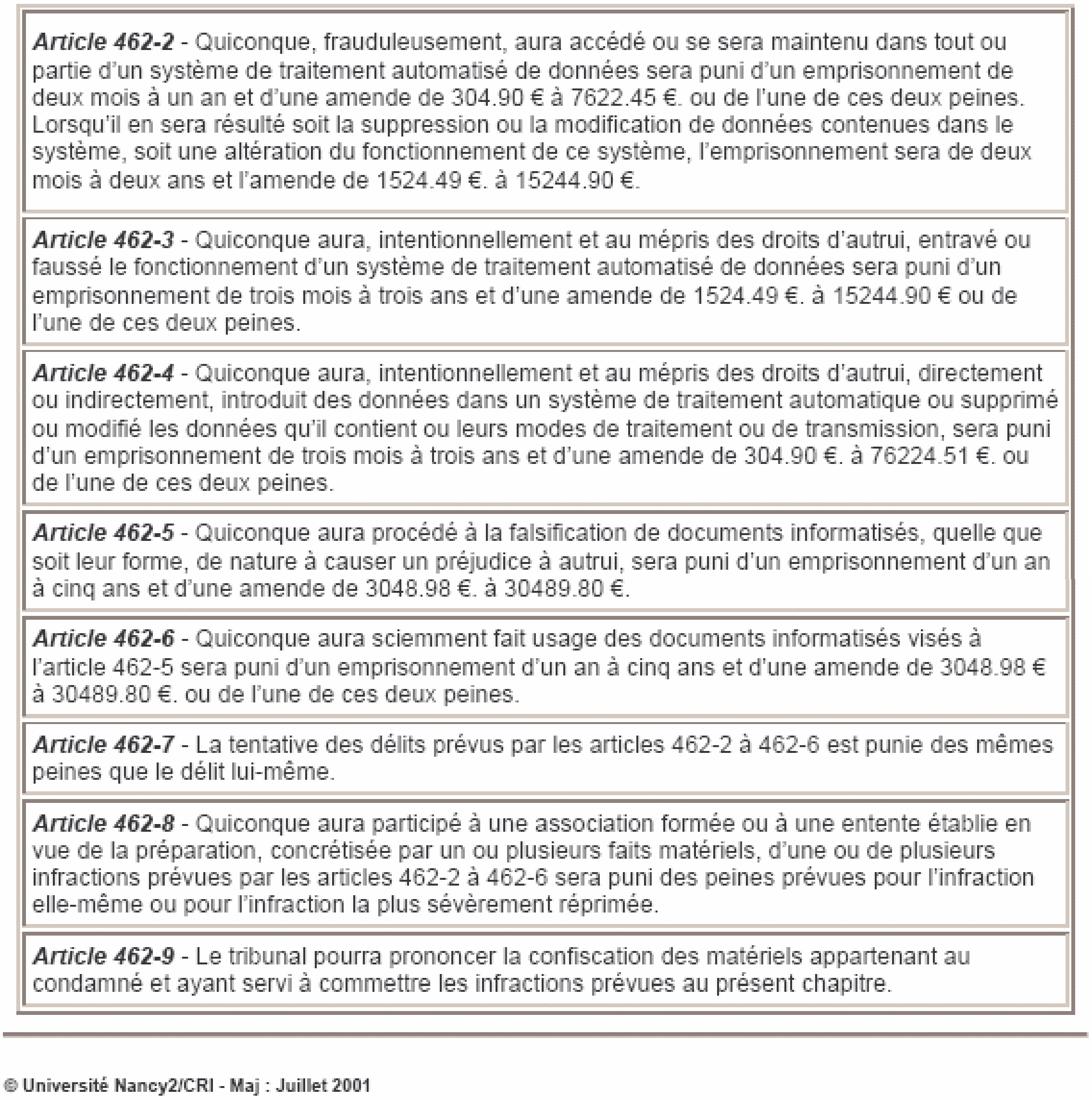


LOI n° 88-19 du 5 Janvier 1988
relative à la fraude informatique

L'Assemblée Nationale et le Sénat ont adopté,
Le Président de la République promulgue la loi dont la teneur suit :

Article unique - Dans le titre II du livre III du code pénal, il est inséré, après le chapitre II, un chapitre III ainsi rédigé :

Chapitre III
De certaines infractions en matière informatique



Article 462-2 - Quiconque, frauduleusement, aura accédé ou se sera maintenu dans tout ou partie d'un système de traitement automatisé de données sera puni d'un emprisonnement de deux mois à un an et d'une amende de 304.90 € à 7622.45 €. ou de l'une de ces deux peines. Lorsqu'il en sera résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, l'emprisonnement sera de deux mois à deux ans et l'amende de 1524.49 €. à 15244.90 €.

Article 462-3 - Quiconque aura, intentionnellement et au mépris des droits d'autrui, entravé ou faussé le fonctionnement d'un système de traitement automatisé de données sera puni d'un emprisonnement de trois mois à trois ans et d'une amende de 1524.49 €. à 15244.90 € ou de l'une de ces deux peines.

Article 462-4 - Quiconque aura, intentionnellement et au mépris des droits d'autrui, directement ou indirectement, introduit des données dans un système de traitement automatique ou supprimé ou modifié les données qu'il contient ou leurs modes de traitement ou de transmission, sera puni d'un emprisonnement de trois mois à trois ans et d'une amende de 304.90 €. à 76224.51 €. ou de l'une de ces deux peines.

Article 462-5 - Quiconque aura procédé à la falsification de documents informatisés, quelle que soit leur forme, de nature à causer un préjudice à autrui, sera puni d'un emprisonnement d'un an à cinq ans et d'une amende de 3048.98 €. à 30489.80 €.

Article 462-6 - Quiconque aura sciemment fait usage des documents informatisés visés à l'article 462-5 sera puni d'un emprisonnement d'un an à cinq ans et d'une amende de 3048.98 € à 30489.80 €. ou de l'une de ces deux peines.

Article 462-7 - La tentative des délits prévus par les articles 462-2 à 462-6 est punie des mêmes peines que le délit lui-même.

Article 462-8 - Quiconque aura participé à une association formée ou à une entente établie en vue de la préparation, concrétisée par un ou plusieurs faits matériels, d'une ou de plusieurs infractions prévues par les articles 462-2 à 462-6 sera puni des peines prévues pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée.

Article 462-9 - Le tribunal pourra prononcer la confiscation des matériels appartenant au condamné et ayant servi à commettre les infractions prévues au présent chapitre.