Charter of proper use of IT systems within École normale supérieure

June 13th, 2016

1.- Fields of application :

This charter, written within the framework of the Policy of Security of Information Systems applies to of the School, all persons using the systems and networks located at the sites of the Ecole Normale Superieure, computer systems that can be accessed from the School and the systems of outside networks at the School, mentioned in the learning of a student or with an agreement with the School.

2.- Access authorization to systems and networks :

2.1. The use of computer resources of the School is subject to prior authorization embodied by opening an account or the right to connect a computer on the network.

2.2. This authorization is strictly personal and can therefore in no case be transferred, even temporarily, to a third party.

2.3. The use of computers is limited to research and education, technical developments, technology transfer, dissemination of scientific, technical and cultural informations, experimentation of new services with technical innovations, but also any administrative or management related to these activities. Without prior authorization, these resources can not be used for projects subject to external funding to the School.

2.4. The School reserves the right to revoke at any time this authorization, without notice.

2.5. This authorization expires upon termination of the activity which justified it. Regarding students, it will terminate within one year after leaving School, unless exceptional reason approved by the Director of the School.

2.6. At the closure of his account, the user may obtain a copy of the contents thereof, except in special cases (clause property, privacy, etc.). The user is responsible before his departure for the destruction of its private data.

2.7. Any connection of personal equipment is subject to authorization and is part of professional practice and safety regulations for the School and its laboratories and departments. The School may not be held liable for theft or damage to equipment belonging to staff, students or visitors.

2.8. In private areas (boarding, lodging), anyone is responsible for the traffic on his Internet connection.

3.- The system administrator :

System administrators are persons who have appointed to install and manage computers. They are responsible to ensure the best possible usage for all.

3.1. The system administrator is subject in the exercise of its functions to a duty of confidentiality. To ensure the smooth operation and security of the system, it may make the necessary investigations. He shall not disclose information acquired by this research except as provided in 3.2.

3.2. In particular it can explore the files and provide extracts to the Direction of departments and School when such research is made necessary by the observation of acts of piracy.

3.3. He can also generate and check all log events, if necessary. The full list of these logs can be accessed by simple request to system administrators.

He can generate statistics for the good management : optimization, security, detection of abuse.

3.4. The system administrator can perform backups of some disks, including those hosting user data and e-mail.

3.5. The administrator can intercept or prohibit any flow (Web, e-mail, file transfer, telephony, video, etc.). presenting security risks (viruses for example) or off charter.

3.6. Security administrators can carry out any research on preventive fault computers, personal or otherwise, connected to the internal network. They can disconnect, physically or logically, computer in case of suspicion.

4.- General safety rules :

All users are responsible for their utilization of resources within the School. They must, at their level, contribute to security. Specially :

4.1. All users must choose strong passwords complying with the recommendations of the system administrator, and the administrator can test their strongness. These passwords must be kept secret, should not be written, should not be stored in systems (excluding strong encryption), and under no case be disclosed to third parties. At the request of system administrators, they must be changed.

4.2. Users should not use accounts other than those for which they received authorization. They must refrain from any attempt to capture or crack the password of another user.

4.3. The use or development programs which intentionnaly undermine the integrity of computer systems within School or on national or international networks are prohibited.

4.4. Any finding of a violation, attempted violation or suspected violation of a system must be reported to security officials of the School.

4.5. Users should not give up their computer without having previously disconnected.

4.6. Users must refrain from any attempt of falsification of identity.

4.7. Users should not add equipment (computer, printer, network switch, wifi access point, ...) without permission. The temporary connection of a computer to a "guest" network is allowed in accordance with the rules relating to these networks.

4.8. Users undertake not to exploit any security holes, malfunctions, defects configuration. They must notify the system administrator, and they should not advertise. The administrator may choose not to make any correction, if the correction is not available or is considered as leading to other problems.

4.9. Users should avoid the introduction and spread of the virus by any means.

4.10. Users must ensure the security of their professional data, including their email, in terms of confidentiality, integrity and availability. This involves ensuring a backup is performed at a frequency according to the need and their storage place is perennial. Encryption is mandatory in the case of mobile computing use (laptops, USB key, PDA, external hard drives, etc.).

The use of external services (disks space, mail, office, etc.) and server data (web, ftp, etc.) having no contractual warranty confidentiality, integrity and availability is prohibited unless express authorization and implementation of adequate protection measures.

When starting a mission, especially abroad, users should note the advice to travelers enacted by ANSSI (use dedicated equipment without sensitive data data without conflict with local laws).

4.11. Users must follow the rules defined by the (eg circular Guyon 4 May 2000 about P2P, CNRS recommendation of 10 August 2005 about Skype, CNRS recommendations of 17 April 2008 for use free services on the Internet, JM.Voltini circular of 16 January 2011 on the disk encryption, etc.).

4.12. Typically, a user must be vigilant and report the system administrators of any anomaly, and comply with their instructions.

4.13. Users must report any theft of computer equipment, personal or professional, to take appropriate actions.

4.14. Users should be careful when connecting to wireless networks poorly secured, including public places.

5.- Use of common resources :

5.1. Any user agrees to use correctly the resources at their disposal : no memory saturation, disk space, network bandwidth, printers, etc. For example, the e-mail chains are prohibited.

5.2. Any user agrees to respect the resources that it is not available to him even if they are available (eg printer).

6.- Respect for intellectual property :

6.1. Reproduction of commercial software other than for creating a backup copy is prohibited.

6.2. It is prohibited to install on any system software, font or any other document in violation of copyrights and licensing rules. The terms of redistribution of free software must be respected.

6.3. Professional software provided by the School on personal machines must be removed when leaving the School.

6.4. The use of library resources must conform to the contract available from the editor and validated by the School. In particular, the massive and systematic downloading of information resources through a robot or any other software is prohibited.

7.- Respect of privacy :

7.1. Any user is responsible, for its files and directories, of access rights to read and modify it gives to other users. However, it is forbidden to look at informations held by other users, even if they are not properly protected. Accordingly, users should not try to read, copy, disclose, modify files of another user without being explicitly permitted.

7.2. Users should not attempt to intercept communications between third parties.

7.3. Users are required to take measures to protect the data ensuring compliance with commitments of confidentiality made by the School with respect to third parties.

7.4. Processing of personal data should remain confidential and in compliance with CNIL declarations.

7.5. In the absence of a user, any measure necessary to the continuity of service can be implemented.

7.6. Users should be extremely vigilant with respect to data considered sensitive under the security policy information systems. In particular, they shall not carry or store without protection (like encryption) any unprotected file of sensitive data on unsecure supports or services. Access to sensitive data is prohibited from positions or untrusted networks. During consultations of sensitive information, users should be alert to the traces left : browsers history, passwords, cache, etc.

8.- Relations with sites :

8.1. It is forbidden to connect or try to connect to another site without being authorized. Anonymous accesses to services (Web, ftp, etc.) are allowed.

8.2. It is forbidden to engage in systems belonging to the School or are connected to the network of the School of acts which intentionnaly compromise the safety or operation of information systems, local or remote, and networks.

8.3. Users must be vigilant when entering any personal information on the Internet, especially with the proliferation of phishing scams. The school will not be liable for damages in such disclosures of information.

8.4. Users connecting somewhere using their identifier Eduroam ENS must respect the rules imposed by the host site.

8.5. External users using eduroam connections offered by ENS undertake to respect this charter and more generally all ENS rules.

9.- Electronic exchanges :

9.1. Within its exchanges, no one can speak on behalf of the School or engage the School without being duly authorized.

9.2. Everyone must exercise the highest standards in respect of its contacts in electronic exchanges.

9.3. Given the legal value of an e-mail, everyone must be vigilant about the content of electronic messages and ensure their conservation.

9.4. It is recalled that any guarantee of transmission can not be given to e-mails that are issued or re-shipped out of the School.

9.5. It is recalled that any publication on a website hosted in the School urges it.

9.6. Use for non-professional topics (forums, blogs or any other publication on the Internet) of professional address should be avoided.

10.- Evolution of the Charter :

This charter is available on the Internet servers of the School, and is subject to changes, according to changing technologies. Only the last French version is authentic, foreign language versions are only informative.

11.- Penalties :

Any user who fail to comply with the provisions of this charter is likely to see suspend its access rights and is liable to prosecution, within the School (disciplinary), civil or criminal (laws of 6 january 1978, of 6 august 2004, and decree 2011-219 25 February 2011), of 4 july 1985, of 5 january 1988, of 4 august 1994, and of 30 december 1990, modified on 26 july 1996, and decree of 17 march 1999, 15 november 2001, 21 june 2004, 3 august 2006, 12 june 2009, of 28 october 2009, and of 14 march 2011.