ÉCOLE
NORMALE
SUPÉRIEURE
DE LYON

15 parvis René-Descartes
BP 7000, 69342 Lyon cedex 07
Tél. +33 (0)4 37 37 60 00
www.ens-lyon.fr

Information Systems Charter ENS de Lyon 2024

Charter validated in CPSI on 03/07/2024 with the following modifications:

- Added mention of the use of 'machine learning' for network intrusion detection.
- Added mention of the use of inventory/automated deployment software on client workstations.

Charter validated in CPSI on 13/12/2021 with the following modifications:

- Added obligation to use the Ens de Lyon antivirus and encryption.
- Addition of the need to comply with RSSI guidelines in the event of an incident.
- Update of legal articles

This Charter defines the General Conditions of Use of the Internet, networks and computing resources within the establishment, specifying the legal frame and the application of the law to help users be aware of their responsibilities.

Preamble

"Information Systems" means all the hardware and software resources that can be made available to the user. For reasons of network security, this also includes the personal equipment of users connected to the network of ENS de Lyon.

"User" means any person having access to computing resources regardless of their status.

Any use that is not defined by the Charter is only tolerated if it remains restricted. Any use for commercial, political or recreational means is prohibited.

Compliance with the law

The internet, networks and digital communication services are not lawless areas. Threats to the core values of education, including in particular the principles of religious, political and commercial neutrality, are also (but not exclusively) banned and if necessary sanctioned by criminal means:

- Infringement of the privacy of others;
- Defamation and insult;
- The provocation of minors to commit illegal or dangerous acts, fostering the corruption of a minor, exploitation of pornographic images of a minor, the dissemination of messages in a violent or pornographic way;
- Provocation to commit a crime and or commit suicide, provocation leading to discrimination, including racial hatred, or violence;
- The reproduction, representation or broadcasting of intellectual work
- Copies of commercial software for any purpose whatsoever, with the exception of a backup copy in the conditions provided for by the code of intellectual property.

Access to computing resources:

The user must respect the terms of connection (wired or wireless) devices to networks as specified by the Information Technology Department (ITD) or local computer technician.

The right of access to computing resources is strictly personal and non-transferable. Users are responsible for the use of computing resources accessed from their personal connection. If the user suspects that his/her password could be compromised, it should immediately be changed.

The IS Department or the local computer technician will not ask for the disclosure a user password.

The right of access is temporary. It is removed in the following cases:

- The function or status no longer justifies it.
- Failure to comply with the Charter.

Access to computing resources is provided to the user for business purposes and for purposes related to pedagogy, research or professional integration. Any stored data is presumed to be professional, unless its file name contains the words "private-personal".

E-mail

E-mail is primarily to exchange information related to the direct activity of the establishment. Any message will be deemed as being related to the institution unless it has a special and explicit reference indicating its private character. The subject of the e-mail correspondence should in this case start with the wording "private-personal".

In legal terms, e-mail messages exchanged with third parties can form a contract, subject to compliance with the conditions laid down by Articles 1366 and 1367 of the civil code. Users must therefore, be vigilant about the nature of the e-mail messages they exchange, as well as for paper mail.

Access to e-mail is granted according to the technical guidance of the IS Department. Giving a password to a third-party to pick up the user's mail is prohibited.

Before the deletion of their account, e-mail account holders will be informed by e-mail. They must then destroy or retrieve their private data.

Wireless networks

Only the IS Department may operate the Hertzian space of ENS de Lyon: apart from this strict framework, it is forbidden to put into operation a wireless access point. Particular attention must be paid to access points that are sometimes enabled by default on the following materials: hotspot, some printers, some network disks.

Commitments of the user:

Users are responsible for their use of computer resources; They must commit to not perform any operations that can affect the operation of the network and the integrity of computer resources.

If they detect a malfunction or security problem, users should immediately alert the IT department or their local computer technician to resolve the problem and if necessary to stop an attack in progress.

When absent from their workstation, users must lock the session.

Any professional Windows or Mac computer connected to the network must have the antivirus provided by Ens de Lyon.

The hard drives of professional workstations must be encrypted (in accordance with the State PSSI and CNRS directives), the user can ask the IT Department or his local IT specialist for this operation.

The user agrees not to install software without ensuring that it is safe.

Users are regularly victims of a phishing and should be particularly vigilant in reading their e-mail

The IT Department can provide a tool to backup workstations. It is up to users to check that this tool works well on their desktop.

Some software and operating systems offer security updates. Users must apply on all equipment connected to the network of Ens de Lyon.

Any experimentation on the security of computer resources and networks, or computer viruses, without prior approval of the head of security (the RSSI) is prohibited.

The user agrees not to access the information of other users on the network. They accept to be monitored following the use of email regarding some general indications of the exchanged message and not its content.

In order to be able to quickly deploy applications or security settings in compliance with the establishment's Information Security Policy (PSSI), system administrators install inventory/automated deployment software on client workstations. These inventory agents only collect technical information about the workstation and are registered with the ENS's

Personal Data Processing Register.

In the event of a compromise, the user accepts that his workstation will be immobilized for the duration of the investigation and undertakes to comply with the instructions of the CISO.

The user may have personal Web pages for professional use. The content of these individual pages is made up by the user under his/her sole responsibility. He is the editor in the sense of the law No. 2004-575 of June 21, 2004. In the event where these pages obviously contain illicit content, ENS de Lyon reserves the right to suspend usage. A report to the public prosecutor will be made under article 40 of the code of criminal procedure.

When the user is required to create files containing personal data, he will ensure compliance with Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 applicable since May 25, 2018 (GDPR) and the law "Informatique et Libertés" of January 6, 1978 amended and in particular to inform the persons concerned in advance as to the purpose and recipients of the processing of this information.
The user must necessarily contact the DPO of ENS de Lyon (dpo@ens-lyon.fr).

Respect of rights:

Respect for intellectual property:

Users must refrain from copying, distributing or reproducing any software or document protected by copyright law. In general, users ensure that what they broadcast on the Internet or data they download does not affect the rights of third parties (copyright, right of brands, right to respect of privacy, etc.).

Respect for the people's rights

It is forbidden for anyone to infringe on the privacy of others through any process, including the transmission without consent of their image or the dissemination of confidential or private written material. In general, the user ensures the respect of the person, privacy and the privacy of others.

Respect of contractual clauses

Users must notably respect contractual obligations concerning the use of electronic documentary resources and notably to use them in a reasonable, personal and strictly non-commercial way.

Correct behaviour

Users must not use the information system to harass other users with unwanted communication from third parties or to display/publicize any illegal information.

Control and traceability

The establishment is under a legal obligation to implement a logging system, archiving Internet access, messaging and exchanged digital communications. These journaling files (called "logs") are processed to improve the security of computing resources or detect misuse of the latter. These "logs" can be made available by judicial application.

These files contain information allowing the identification of the user, the data related to the equipment used, date, time and duration of each communication, data relating to the additional services requested or used and their suppliers, to identify the recipients. Logs can be kept for up to one year.

The establishment implements "intrusion detection" systems, notably based on "machine learning," which analyze network traffic in real-time and alert the Chief Information Security Officer (CISO) of any potential signs of a hacking attempt

Continuous service, management of absences and departures

Users are responsible for their private data. Upon their departure, they must destroy their data. Business data must be stored on shared spaces: shared folders per department, or boxes per facility.

Protection of the personal data

In accordance with the law "Informatique et Libertés" of January 6, 1978 as amended, Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 applicable since May 25, 2018 (RGPD) and the law of June 21, 2014 for confidence in the Digital Economy, ENS de Lyon undertakes to comply with the regulations in force applicable to the processing of personal data.

In accordance with the legal and regulatory provisions in force, the user whose personal data is collected has the right to access, rectify, update and delete information concerning him, which he can exercise in by writing to dpo@ens-lyon.fr

The President of ENS de Lyon is responsible for processing.

The legal basis for the processing is based on the performance of a task in the public interest.

ENS de Lyon notably guarantees the user:

- to use the personal data concerning him only for the strict purposes for which they are collected (opening of the Access Account, technical checks, etc.);
- a retention period for personal data which cannot exceed what is necessary to achieve the purposes for which they are collected.

ENS de Lyon undertakes to take all the necessary precautions to preserve the security of this personal data and in particular that it is not communicated to unauthorized persons.

Legal reminders

Users are required to comply with the legislation in force:

• Respect for people (no invasion of privacy or secrecy of correspondence, nor insults or defamation) and respect for information systems:

- Article 9 of the Civil Code
- Articles 226-1, 226-15, 222-17, R 621-2, 226-10 of the Criminal Code
- Law No. 2004-669 of July 9, 2004
- Articles 26, 27,34, 36 of Law No. 78-17 of January 6, 1978
- Articles 313-1 and following 323-1 to 323-7 of the Penal Code

• The protection of minors against content that is degrading, violent or promotes its corruption:

- Articles 227-24, 227-23 of the Penal Code
- Law 2004-575 of June 21, 2004

• Crimes and misdemeanors committed through the press or by any other means of publication:

- Articles 23 to 41-1 of the Law of July 29, 1881

• Respect for the copyright of literary, musical, photographic or audiovisual works posted online, respect for intellectual property for software

- Articles L 335-3, L 111-1, L 121-1, L 122-1, L 123-2, L 131-2 of the Intellectual Property Code

• Protection against computer crimes (unauthorized entry into an automated system, destruction or modification of data, fraudulent introduction of data, obstruction of operation):

- Articles 323-1 to 323-8 of the Penal Code

• Retention of connection data:

- Article R.10-13 Post and Electronic Communications Code

• Protection of personal data:

- "Computing and Liberties" law of January 6, 1978
- Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 applicable since May 25, 2018 (GDPR)
- Law of June 21, 2014 for confidence in the Digital Economy