Observatoire des Sciences de l'Univers de Lyon

Engagement à respecter la charte informatique

Je soussigné(e) :

Nom :

Prénom :

Statut :

- ○ Permanent ;
- ○ Doctorant ;
- ○ ATER ;
- ○ Post-doctorant ;
- ○ Stagiaire ;
- ○ Autre :

Votre responsable au sein de l'unité :

Votre adresse électronique personnelle :

Reconnais avoir pris connaissance de la charte informatique fournie :

- ☐ Charte pour l'utilisation des ressources informatiques de l'UCBL, version du 19/12/2017 ;
- ☐ Charte d'usage du SI de l'ENS de Lyon, version du 13/12/2021 ;
- ☐ IS charter ENS de Lyon, version du 13/12/2021 ;
- ☐ Top 10 Secure Computing Tips du RSSI de l'UCBL ;

Seuls les ordinateurs de l'administration ou professionnels sont autorisés à se connecter au réseau filaire de l'unité.

Je m'engage à la respecter.

Fait à Lyon, le

Signature de l'intéressé(e), précédé de la mention « Lu et approuvé ».

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

Charte d'usage du Système d'Information ENS de Lyon 2022

Charte validée en CPSI le 13/12/2021 avec les modifications suivantes :

- Ajout obligation de l'utilisation de l'antivirus Ens de Lyon et chiffrement.
- Ajout nécessité de se conformer aux consignes RSSI en cas d'incident.
- Mise à jour des articles juridiques

La Charte définit les conditions générales d'utilisation de l'Internet, des réseaux et des ressources informatiques au sein de l'établissement, en rappelant l'application du droit et en précisant le cadre légal afin de sensibiliser et de responsabiliser l'utilisateur.

Préambule

Par "Système d'Information" s'entend l'ensemble des moyens matériels et logiciels pouvant être mis à disposition de l'utilisateur. Pour des raisons de sécurité du réseau, cela inclut également le matériel personnel des utilisateurs connecté au réseau de l'ENS de Lyon.

Par "utilisateur" s'entend toute personne ayant accès aux ressources informatiques quel que soit son statut.

Les usages non définis par la Charte ne sont tolérés que s'ils s'exercent de manière résiduelle. Toute utilisation à des fins commerciales, politiques ou ludiques est interdite.

Respect de la législation

L'internet, les réseaux et les services de communication numérique ne sont pas des zones de non droit. Outre l'atteinte aux valeurs fondamentales de l'Éducation Nationale et l'ESR, dont en particulier les principes de neutralité religieuse, politique et commerciale, sont également (mais pas exclusivement) interdits et le cas échéant sanctionnés par voie pénale :

- L'atteinte à la vie privée d'autrui ;
- La diffamation et l'injure ;
- La provocation de mineurs à commettre des actes illicites ou dangereux, le fait de favoriser la corruption d'un mineur, l'exploitation à caractère pornographique de l'image d'un mineur, la diffusion de messages à caractère violent ou pornographique ;

- La provocation aux crimes et délits et la provocation au suicide, la provocation à la discrimination, à la haine notamment raciale, ou à la violence ;
- La reproduction, représentation ou diffusion d'une œuvre de l'esprit ;
- Les copies de logiciels commerciaux pour quelque usage que ce soit, hormis une copie de sauvegarde dans les conditions prévues par le code de la propriété intellectuelle.

Accès aux ressources informatiques :

L'utilisateur doit respecter les modalités de raccordement (filaire ou sans fil) des matériels aux réseaux telles qu'elles lui sont précisées par la Direction des Systèmes d'Information (DSI) ou son informaticien de proximité.

Le droit d'accès aux ressources informatiques est strictement personnel, incessible et non transférable. L'utilisateur est responsable de l'utilisation des ressources informatiques effectuée à partir de son droit d'accès. Si l'utilisateur a un doute sur le fait que son mot de passe ait pu être compromis, il doit immédiatement le changer.

La DSI ou l'informaticien de proximité ne demanderont en aucun cas la communication du mot de passe d'un utilisateur.

Le droit d'accès est temporaire.

Il est retiré dans les cas suivants :

- La fonction ou le statut ne le justifie plus
- Non-respect de la présente charte.

L'accès aux ressources informatiques est fourni à l'utilisateur à des fins professionnelles et à des fins liées à la pédagogie, à la recherche ou à l'insertion professionnelle. Toute donnée stockée est présumée professionnelle, sauf si son nom contient « privé-personnel ».

Messagerie électronique

La messagerie électronique permet principalement d'échanger les informations à vocation liées à l'activité directe de l'établissement. Tout message sera réputé lié à l'institution sauf s'il comporte une mention particulière et explicite indiquant son caractère privé. Le sujet de la correspondance électronique devra alors commencer pas la mention "privé-personnel".

Les messages électroniques échangés avec des tiers peuvent, au plan juridique, former un contrat, sous réserve du respect des conditions fixées par les articles 1366 et 1367 du code civil. L'utilisateur doit en conséquence, être vigilant sur la nature des messages électroniques qu'il échange au même titre que pour les courriers papier.

L'accès à la messagerie électronique se fait selon les indications techniques de la DSI. L'usage de systèmes consistant à remettre son mot de passe à un opérateur tiers pour relever son courrier est interdit.

Avant la suppression de son compte, le titulaire du compte de messagerie est informé par message électronique. Il lui appartient alors de détruire ou récupérer ses données à caractère privé.

Réseaux sans-fil

Seule la DSI exploite l'espace hertzien de l'établissement : en dehors de ce cadre strict, il est interdit de mettre en exploitation un point d'accès sans fil. Attention des points d'accès sont parfois activés par défaut sur les matériels suivants : borne wifi, certaines imprimantes, certains disques réseaux.

Engagements de l'utilisateur :

Tout utilisateur est responsable de son utilisation des ressources informatiques ; Il s'engage à ne pas effectuer d'opérations pouvant nuire au fonctionnement du réseau et à l'intégrité des ressources informatiques.

S'il constate un dysfonctionnement ou problème de sécurité, l'utilisateur doit alerter immédiatement la DSI ou son informaticien de proximité afin de permettre la résolution du problème et éventuellement arrêter une attaque en cours.

S'il s'absente de son poste de travail l'utilisateur doit verrouiller sa session.

Tout poste professionnel Windows ou Mac connecté au réseau doit être équipé de l'antivirus fourni par l'Ens de Lyon.

Les disques durs des postes professionnels doivent être chiffrés (conformément à la PSSI Etat et aux directives du CNRS), l'utilisateur peut se rapprocher de la DSI ou de son informaticien de proximité pour cette opération.

L'utilisateur s'engage à ne pas installer de logiciels sans s'assurer de l'innocuité de ceux-ci.

Chaque utilisateur est victime de tentative d'hameçonnage régulière, il convient d'être particulièrement vigilant à la lecture de sa messagerie électronique.

La DSI peut mettre à disposition un outil de sauvegarde des postes de travail. Il incombe à l'utilisateur de vérifier que cet outil fonctionne bien sur son poste.

Les systèmes d'exploitation et certains logiciels proposent des mises à jour de sécurité. Les utilisateurs doivent les appliquer sur tout équipement connecté au réseau de l'ENS de Lyon.

Toute expérimentation sur la sécurité des ressources informatiques et réseaux ou sur les virus informatiques, sans autorisation préalable du Responsable de la Sécurité du Système d'Information (RSSI), est interdite.

L'utilisateur s'engage à ne pas accéder aux informations d'autres utilisateurs sur le réseau. Il accepte un contrôle à posteriori de l'utilisation de sa messagerie qui ne pourra porter que sur des indications générales du message échangé et non sur son contenu.

En cas de compromission, l'utilisateur accepte que son poste soit immobilisé le temps de l'enquête et s'engage à respecter les consignes du RSSI.

L'utilisateur peut disposer des pages Web personnelles à usage professionnel. Le contenu de ces pages professionnelles individuelles est réalisé par l'utilisateur, sous sa seule responsabilité. Il en est l'éditeur au sens de la loi n° 2004-575 du 21 juin 2004. Dans l'hypothèse où ces pages abriteraient des contenus manifestement illicites, l'établissement se réserve le droit d'en suspendre l'usage. Un signalement au procureur de la République sera effectué au titre de l'article 40 du code de procédure pénale. Lorsque l'utilisateur est amené à constituer des fichiers comportant des données à caractère personnel, il veillera à respecter le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 applicable depuis le 25 mai 2018 (RGPD) et la loi *« informatique et libertés »* du 6 janvier 1978 modifiée et notamment procéder à l'information préalable des personnes concernées quant à la finalité et les destinataires du traitement de ces informations. L'utilisateur devra nécessairement contacter le DPO de l'ENS de Lyon (dpo@ens-lyon.fr).

Respect des droits :

Respect de la propriété intellectuelle :

Les utilisateurs doivent s'abstenir de copier, diffuser ou reproduire tout logiciel ou document protégé par le droit d'auteur. De manière générale, les utilisateurs s'assurent que les données qu'ils diffusent sur Internet ou qu'ils téléchargent ne portent pas atteinte aux droits des tiers (droit d'auteur, droit des marques, droit au respect de la vie privée etc.).

Respect du droit des personnes

Il est interdit à tout utilisateur de porter atteinte à la vie privée d'autrui par un procédé quelconque et notamment par la transmission sans son consentement de son image ou de ses écrits diffusés à titre confidentiel ou privé. De manière générale, l'utilisateur veille au respect de la personne, de l'intimité et de la vie privée d'autrui.

Respect des clauses contractuelles

Les utilisateurs doivent notamment respecter les conditions contractuelles prévues pour l'usage des ressources documentaires électroniques et notamment en avoir un usage raisonnable, personnel et strictement non commercial.

Comportement approprié

Un utilisateur ne doit pas utiliser les systèmes informatiques pour harceler d'autres utilisateurs par des communications non souhaitées par les tiers ou pour afficher/diffuser des informations illégales.

Contrôle et traçabilité

L'établissement est dans l'obligation légale de mettre en place un système de journalisation, archivage des accès Internet, de la messagerie et des communications numériques échangées. Ces fichiers de journalisation (appelé "logs") sont traités pour améliorer la sécurité des ressources informatiques ou détecter des abus. Ces "logs" peuvent être mis à disposition sur réquisition judiciaire.

Ces fichiers comportent les informations permettant l'identification de l'utilisateur, les données relatives aux équipements utilisés, date, heure et durée de chaque communication, données relatives aux services complémentaires demandés ou utilisés et leurs fournisseurs, données permettant d'identifier le ou les destinataires. La durée de conservation des journaux informatiques est d'un an maximum.

L'établissement met en œuvre un système de « détection d'intrusion » qui analyse en temps réel le trafic réseau et signale au RSSI les éventuels signes d'une tentative de piratage.

Continuité de service, gestion absences et départs

L'utilisateur est responsable de ses données à caractère privé. Lors de son départ, il lui appartient de détruire ses données. Les données professionnelles doivent être stockées sur des espaces mutualisés : dossiers partagés de services, boîtes de fonction.

Protection des données à caractère personnel

Conformément à la loi *« informatique et libertés »* du 6 janvier 1978 modifiée, au règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 applicable depuis le 25 mai 2018 (RGPD) et à la loi du 21 Juin 2014 pour la confiance dans l'Économie Numérique, l'ENS de Lyon s'engage à respecter la réglementation en vigueur applicable au traitement de données à caractère personnel.

Conformément aux dispositions légales et réglementaires en vigueur, l'utilisateur dont les données personnelles sont collectées bénéficie d'un droit d'accès, de rectification, de mise à jour et d'effacement des informations le concernant, qu'il peut exercer en s'adressant à dpo@ens-lyon.fr

Le Président de l'ENS de Lyon est le responsable des traitements.

La base légale du traitement repose sur l'exécution d'une mission d'intérêt public.

L'ENS de Lyon garantit notamment à l'utilisateur :

- de n'utiliser les données à caractère personnel le concernant que pour les strictes finalités pour lesquelles elles sont collectées (ouverture du Compte d'accès, contrôles techniques, etc.) ;

- une durée de conservation des données personnelles qui ne peut pas excéder ce qui est nécessaire à la réalisation des finalités pour lesquelles elles sont collectées.

L'ENS de Lyon s'engage à prendre toutes les précautions nécessaires afin de préserver la sécurité de ces données personnelles et notamment qu'elles ne soient pas communiquées à des personnes non autorisées.

Rappels juridiques

Les utilisateurs sont tenus de respecter la législation en vigueur :

➢ *Le respect des personnes (pas d'atteinte à la vie privée ou au secret de la correspondance, ni d'injures ou de diffamation) et respect des systèmes d'informations :*

- Article 9 du Code civil
- Articles 226-1,226-15, 222-17, R 621-2, 226-10 du Code pénal
- Loi nº 2004-669 du 9 juillet 2004
- Articles 26, 27,34, 36 de la Loi n° 78-17 du 6 janvier 1978
- Articles 313-1 et suite 323-1 à 323-7 du Code pénal

➢ *La protection des mineurs contre les contenus dégradants, violents ou favorisant sa corruption* :

- Article 227-24, 227-23 du Code pénal
- Loi 2004- 575 du 21 juin 2004

➢ *Des crimes et délits commis par la voie de la presse ou par tout autre moyen de publication :*

- Articles 23 à 41-1 de la Loi du 29 juillet 1881

➢ *Le respect du droit d'auteur des œuvres littéraires, musicales, photographiques ou audiovisuelles mises en ligne, respect de la propriété intellectuelle pour les logiciels.*

- Articles L 335-3, L 111-1, L 121-1, L 122-1, L 123-2, L 131-2 du Code de propriété intellectuelle

➢ *Protection contre les délits informatiques (pénétration non autorisée sur un système automatisé, destruction ou modification de données, introduction frauduleuse d données, entrave au fonctionnement)* :

- Articles 323-1 à 323-8 du Code pénal

➢ *Conservation des données de connexion* :

- Article R.10-13 Code des postes et des communications électroniques

➢ *Protection des données à caractère personnel :*

- *Loi « informatique et libertés » du 6 janvier 1978*
- *Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 applicable depuis le 25 mai 2018 (RGPD)*
- *Loi du 21 Juin 2014 pour la confiance dans l'Économie Numérique*

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 2022

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 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 uses a system of "intrusion detection" which analyzes real-time network traffic and alerts the RSSI 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