Internal Rules of Rézo Metz

validated by the general meeting held on January 14, 2021 in Metz

Préambule

This document aims to define the various rules to be respected by all persons within the Rézo Metz association, in accordance with its current statutes. Reference will be made to the members of the association, designated by the term « members », to the Rézo Metz association, designated by the term « Rézo », and to the École CentraleSupélec, and designated by the latter name.

In the event of disagreement between this document and the Articles of Association, the latter shall prevail. In case of a difference between the French version and this translation despite our efforts to translate it faithfully, the French version prevails.

Article 1 : Membership

Article 1-1 : Membership fee

. To become a member of Rézo, the interested person must pay a membership fee. This amounts to :
— 2 euros for a one-week membership ;
— 5 euros for a one-month membership ;
— 25 euros for a six-month membership ;
— 40 euros for a one-year membership ;
The payment of a membership fee can be made by cheque, cash, bank transfer or credit card. Once acquired, the membership fee can only be refunded by decision of the Steering Committee.

Definitive membership is decided by the Steering Committee after full payment of the membership fee.

Article 1-2 : Exemption from membership fee

The following are exempt from paying contributions
— members of honours ;
— benefactor members.

In addition, a person in financial difficulty may be exempted from paying contributions. A reasoned request must be addressed to the Seetring Committee, accompanied by the necessary evidence for the Steering Committee to make a decision. In addition, an oral interview may take place. The Steering Committee shall decide on the application within 7 days.

The person will be considered a full member of the association and will enjoy all associated rights in the same way as other members.

Article 2 : Services offered by the association

Article 2-1 : Available services

The main service the association offers its members is internet access. This access manifests itself as follows :

— Each room is equipped with a RJ-45 ethernet socket connected to Rézo ;

— A WiFi network is deployed in a large part of the residence.

The association offers other secondary services, a list of which can be found on the association's website.

Article 2-2 : Modification of services

Le Rézo reserves the right to modify at any time the services offered and the rules in force on the network. Any member who would not be satisfied by these new rules can obtain his disconnection with partial reimbursement on the advice of the Steering Committee.

Article 3 : Conditions of access to the services

Access to the WiFi internet network « FedeRez » is granted to all members of the FedeRez association. The rules of procedure then apply, even if the person is not a member of the Rézo.

The Steering Committee may grant exemptions from membership fees (free access) to members and former members of Rézo, in particular and specific cases, at its discretion. The rules of procedure apply even if the person is no longer a member of Rézo.

Apart from these exceptions, the member must, in order to access the services described in article 2, be up to date with his or her membership fees.

In all cases, any person using the services of Rézo must respect the commitments described in article 4.

Access to the Internet is subject to the registration of the machines on the management software of Rézo. The registration of a machine includes in particular the registration of its MAC address. Registration can be automatic or manual. Unless otherwise agreed, each member is limited to 10 machines registered simultaneously on his account.

Article 4 : Commitments of the members towards the association

Article 4-1 : RENATER and CentraleSupélec charters

The RENATER network is the National Telecommunications Network for Technology, Education and Research. It provides a connection to the CentraleSupélec school, the latter providing our internet access.

Thus, any member of the association must, even if he or she is not a student at CentraleSupélec, accept the RENATER charter and the CentraleSupélec charter, which are given in the appendix to the present internal rules.

In the event of disagreement between the rules and one of the two charters, the charters shall prevail.

These charters include (but are not limited to) the following restrictions :

— the obligation to have antivirus software installed, up to date, and in operation as soon as the machine is started ;

— the prohibition to install server-type software on its machine which is directly accessible outside the local network of the residence. These terms include HTTP or FTP servers ;

— It is prohibited to send or receive files in violation of copying laws, especially by using the exchange networks known as « Peer to Peer » or « P2P », but also via HTTP, FTP, IRC, etc. A non-exhaustive list of software whose use is prohibited is available on the association's internal website ;

— More generally, it is forbidden to infringe French law, in particular with regard to information systems.

Article 4-2 : Automatic configuration

. When wired or wirelessly connecting to the Rezo, an automatic configuration is applied to the machine. The machine includes :
— the IP address ;
— he subnet mask ;
— the default gateway.
Any member undertakes not to modify this configuration without the agreement of an active member of Rézo.

Any member also undertakes not to voluntarily modify the physical addresses, in particular the MAC addresses, of its network interfaces without the agreement of an active member of Rézo.

Article 4-3 : Use of routers

Every member undertakes not to connect a router without the agreement of an active member of Rézo. It should be noted that most WiFi terminals are equipped with an internal router and are subject to this rule.

However, it should be noted that in the parts of the residence where the WiFi network is weak or non-existent, an exemption could be granted taking into account the following points :
— in accordance with article 4-4, only the interested member could benefit from the WiFi network ;
— the installation of the terminal must not interfere with the existing WiFi network ;
— The member must remain in control of his installation at all times,
— Rézo may at any time, and without prior notice, withdraw its exemption, in particular in cases where one of the conditions below is no longer met.

Article 4-4 : Account Sharing

Is considered as account sharing :
— the voluntary sharing of its login identifiers to a person member or non-member of Rézo ;
— the registration of a machine which is not his.
Account sharing is strictly forbidden.

The member is also invited to choose a strong password on the management site.

Article 4-5 : Control of his devices

By joining the association, the member releases Rézo from any responsibility for the activities carried out by the member, and accepts full responsibility for them.

Furthermore, membership of Rézo implies the respect of the following rules :
— control at all times the flows emitted or received by its machine, be aware of the services installed, and not leave its machine unattended. The member will be held responsible for any offence committed from his machine ;
— not to use software affecting the quality of service or security on the network (in particular those containing spyware) ;
— not to send unsolicited e-mail (spam), in particular not to transfer or send messages of dubious origin, advertising or political, religious or commercial propaganda.

Article 4-6 : Viruses

Under no circumstances is Rézo responsible for any damage to the member's machine, whether it is a virus infection or any other type of attack. The member is invited to take all necessary precautions

in order not to compromise his machine or those of other members. It should be noted that in case of infection by a virus, Rézo reserves the right to suspend the internet action for the said machine. Access will be restored only after verification by an active member of Rézo that the machine is no longer infected (the cleaning of viruses remains the responsibility of the owner).

Article 5 : Commitments of the association towards the members

Article 5-1 : Support

Rézo undertakes to provide technical and administrative support as best it can according to the means of contact set out in article 5-4.

Rézo may also, subject to the availability of staff, provide support in the form of on-call services.

Article 5-2 : Availability

Rézo is committed to maintaining optimal availability of its services. These may be interrupted, in particular in the event of maintenance or malfunction.

In the event that internet access is not possible for a member, the latter can receive, on simple request, a certificate from the association with, in particular, the dates on which the member did not have access to the internet.

If Internet access is severely disrupted for more than one week (minimum subscription period), refunds may be made, on the advice of the Steering Committee.

Article 5-3 : Prevention of maintenance

Rézo tries, as far as possible, to inform the members of the association of any maintenance by e-mail.

Article 5-4 : Contacts

Rézo is contactable with the following means :
- By mail :
  Association Rézo Metz École CentraleSupélec 2 rue Édouard Belin 57070 Metz
- By e-mail
  - rezo-admin@rezometz.org for technical questions
  - bureau@rezometz.org for administrative matters
  - contact@rezometz.org for other questions
- By tickets, on the management site https ://re2o.rezometz.org for technical problems.

Article 6 : Lending of equipment

Article 6-1 : Equipment concerned

On certain occasions, Rézo can lend equipment to its members. This material includes, but is not limited to, :
- of RJ45 ethernet cables ;
- USB-RJ45 adapters ;
- Individual WiFi terminals.

Article 6-2 : Loan conditions

The member undertakes to :

— Do not damage the equipment on loan ;
— To return the equipment lent at the end of its period of contribution, or if necessary, of the loan contract.

Rézo will be able to set up a guarantee and a loan contract in cases where it deems it necessary.

Article 6-3 : Case of WiFi terminals in the apartments

In the flats in building A (A001, A101, A201, A301) and C (C001, C101, C201, C301), a WiFi terminal is installed in the corridor cupboard. These terminals, in addition to providing WiFi access to the inhabitants of the flat, also provide access to some inhabitants in the corridors outside the flats.

The inhabitants of the flat must not, without prior authorisation from Rézo, alter the correct operation of the terminal and in particular must not disconnect it.

Additional provisions with regard to these bollards may be set by agreement with the OPHMM.

Article 7 : Data Protection Act and RGPD

Article 7-1 : Confidentiality of data

Rézo reserves the right to analyse by automated processing the traffic of members for the purposes of flow regulation, security checks and verification of the application of these rules. The data collected may only be consulted by the Steering Committee, by persons designated by the latter, and by the judicial authorities. The persons having access to these data have undertaken in writing to respect the privacy of users and not to disclose this information to persons who are not members of the Steering Committee.

Article 7-2 : Rezo's commitments towards the user

According to the French Data Protection Act and the RGPD, members have the right to access, rectify, inform and oppose data concerning them. This right can be exercised by e-mail, in person by post with the contacts listed in article 5-4. All requests must be accompanied by proof of identity.

Article 8 : Penalties

The governing bodies of Rézo, validly convened in disciplinary formations, are authorised to impose sanctions on its members in the event of non-compliance with the Articles of Association or the internal rules or any attempt to circumvent the rules or limitations imposed by Rézo. These may go as far as the temporary suspension of digital services or permanent exclusion.

In accordance with the statutes in force, the interested member is however invited to present its written and, if it so wishes, oral observations to the Steering Committee. The decision is nevertheless left to the discretion of the Rézo Steering Committee.

Rézo remains at the disposal of its members for any further information.

In accordance with the articles of association in force, this document may only be modified by the general meeting, with the exception of the appendices, which may be updated by the Steering Committee after simple notification by e-mail to members, in the event that CentraleSupélec and/or RENATER make changes to the charters.

Made in Metz, on January 14, 2021 in three original copies.

On behalf of the members of the General Meeting of Rézo Metz,

President
Yoann Piétri

Secretary
Achille Depoix

A Charte RENATER

RENATER
CONNECTEUR DE SAVOIRS

CHARTE DE BON USAGE DE L'INFORMATIQUE ET DU RESEAU RENATER

La présente charte a pour objet de définir les conditions d'accès et les règles d'utilisation des outils informatiques et de l'accès à Internet mis à la disposition des utilisateurs par [l'université ou le CROUS de ……].

Le réseau informatique de [l'université ou du CROUS de ……] est relié par l'intermédiaire du Réseau RENATER (Réseau National de télécommunications pour la Technologie, l'Enseignement et la Recherche) à une communauté d'utilisateurs travaillant dans le domaine de l'éducation, de la recherche et de la technologie.

Le réseau RENATER a pour objet de ne véhiculer que le trafic engendré par ces activités de recherche, de développement technologique et d'éducation.

Les ressources informatiques et les services Internet de [l'université ou du CROUS de ……] sont mis à la disposition des utilisateurs à des fins d'enseignement, de culture, de recherche et de diffusion d'informations scientifiques et pédagogiques.

Etant donné qu'un réseau est caractérisé par l'interdépendance de ses utilisateurs, un trouble ou acte malveillant peut atteindre toute la communauté. Pour le bon fonctionnement du réseau et le respect de ses utilisateurs, [l'université ou le CROUS de ……] souscrit à un code de bonne conduite à respecter en matière d'utilisation d'Internet.

Pour accéder aux services de RENATER, les utilisateurs individuels doivent s'engager sur les termes de la présente charte.

* * *

I Principes à respecter :

1/ Finalité de l'utilisation

L'accès aux moyens informatiques et à l'Internet est strictement personnel et incessible. Cet accès est à des fins professionnelles, à savoir enseignement, recherche, développements techniques, transfert de technologies, diffusion d'informations scientifiques, techniques et culturelles, expérimentations de nouveaux services présentant un caractère d'innovation technique.

A ce titre, est interdite toute utilisation des ressources informatiques et d'Internet via RENATER à des fins commerciales, personnelles (autres que dans le cadre d'activités de recherche ou de formation, de culture ou de recherche), ou à des fins ludiques (jeux multimédia « en réseau » ou autres).

Il est interdit à l'utilisateur de donner accès à titre commercial ou non, rémunéré ou non, au réseau RENATER à des tiers.

2/ Utilisation loyale du réseau

Toute opération offerte au public, sous quelle que dénomination que ce soit, pour faire naître l'espérance d'un gain qui serait acquis par la voie du sort, notamment les loteries, est strictement interdite.

Tout utilisateur est responsable de l'utilisation rationnelle des ressources du réseau auquel il a accès de manière à éviter toute consommation abusive et/ou détournée de ces ressources.

Plus particulièrement, il doit :

* S'abstenir de toute utilisation malveillante destinée à perturber ou porter atteinte au réseau auquel il a accès.
* Utiliser de manière loyale le réseau en évitant de créer ou de générer des données ayant pour effet la saturation du réseau ou encore épuiser les ressources de ses équipements.
* Appliquer les recommandations de sécurité de l'établissement qui permet le raccordement,
* Signaler toute tentative de violation de son compte, ou d'intrusion sur ses équipements.

3/ Licéité du contenu échangé

a. Respect du droit à la propriété « intellectuelle »

Les données diffusées sur Internet doivent avoir été obtenues licitement et ne pas porter atteinte au droit des tiers.
L'utilisateur des ressources informatiques et d'Internet doit veiller au respect du droit de propriété d'autrui, et plus particulièrement :

* L'utilisation des logiciels sur le réseau ou sur des machines indépendantes s'effectue dans le respect des termes de la licence d'utilisation,
* Il s'interdit la reproduction des logiciels commerciaux autre que pour l'établissement d'une copie de sauvegarde,
* Il respecte les droits de propriété intellectuelle sur des œuvres protégées (livres, logos, pièces musicales, images, logiciels…), qui font interdiction d'utiliser, de reproduire et d'exploiter ces œuvres sans l'autorisation de l'auteur ou du titulaire des droits.

b. 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 personnalité, de l'intimité et de la vie privée d'autrui, y compris des mineurs.

c. Respect de l'ordre public

RENATER ne saurait être un vecteur de la provocation et à ce titre, l'utilisateur agit dans le respect de l'ordre public et s'interdit notamment toute provocation à un acte malveillant de quelle que nature que

ce soit (trouble à l'ordre public, incitation au racisme, incitation au terrorisme, incitation au suicide) ou toute diffusion de message à caractère violent de nature à porter atteinte à la dignité humaine.

4/ Confidentialité

L'utilisateur respecte les contenus à caractère confidentiel, et s'engage particulièrement :

- A ne pas lire, copier, divulguer ou modifier les fichiers d'un autre utilisateur sans y avoir été explicitement autorisé par son propriétaire et/ou son auteur,

- A ne pas intercepter les communications entre tiers.

II Sanctions encourues :

L'utilisateur qui enfreint une des règles énoncées dans la présente charte encoure d'éventuelles sanctions disciplinaires et/ou la suppression de son accès aux ressources RENATER.

Par ailleurs, il peut faire l'objet de poursuites pénales.

Engagement personnel de l'utilisateur

Je, soussigné(e)……, demeurant à…….. , déclare avoir pris connaissance des dispositions de la présente charte, et m'engage à les respecter. Dans le cas contraire, je ne pourrais pas m'opposer à la suppression de mon accès à RENATER.

A……le…….

Signature :

B Charte RENATER

Version: 2014

Charte déontologique RENATER

1. La présente Charte déontologique définit les règles d'usage qui s'imposent à tout utilisateur du Réseau RENATER[1].

2. Le réseau RENATER est un réseau qui, par nature, recèle des risques dont l'Etablissement Signataire est informé. Il est nécessairement utilisé sous la responsabilité du Signataire.

   Il appelle pour son bon usage et sa sécurité, une coopération entre les utilisateurs. Celle-ci repose notamment sur l'engagement de l'Etablissement Signataire, au nom des utilisateurs de son/ses Sites[2] ayant accès directement ou indirectement au réseau RENATER, à veiller à :

   - une utilisation à des fins strictement professionnelles conforme à la finalité du réseau RENATER : enseignement, recherche, développements techniques, transfert de technologies, diffusion d'informations scientifiques, techniques et culturelles, expérimentations de nouveaux services présentant un caractère d'innovation technique (voir annexe 1, point 1) ;

   - une utilisation rationnelle des ressources du réseau RENATER de manière à éviter toute consommation abusive de ces ressources, notamment en soumettant à l'agrément préalable du GIP RENATER la mise en oeuvre d'applications qui engendrent un trafic permanent (voir annexe 1, point 2) ;

   - une utilisation loyale des ressources du réseau RENATER en prévenant et s'abstenant de toute utilisation malveillante destinée à perturber ou porter atteinte au réseau RENATER (voir annexe 1, point 3) ;

[1] L'expression "réseau RENATER" désigne l'ensemble des réseaux ou nœuds de communication délivrant directement ou indirectement, sur le territoire national, aux sites agréés, tout ou partie des services pour lesquels le GIP RENATER est maître d'ouvrage, quel qu'en soit l'opérateur ou le maître d'œuvre.

[2] Le(s) Site(s) du Signataire désigne(nt) le ou les sites à l'intérieur duquel/desquels toutes les entités (bâtiments, étages, locaux etc.) reliées, directement ou indirectement, au réseau RENATER relèvent de la personne morale représentée par le Signataire de la présente Charte.

- véhiculer et mettre à disposition sur le réseau seulement des données licites au regard des lois qui leur sont applicables (voir annexe 1, point 4 et annexe 4 : liste informative et non exhaustive pour ce qui concerne les lois françaises) ;

- ne pas donner accès à titre commercial ou non, rémunéré ou non, au réseau RENATER à des tiers non autorisés sans l'accord préalable et exprès du GIP RENATER (voir annexe 1, point 5) ;

- mettre en oeuvre les ressources techniques et humaines requises pour assurer un niveau permanent de sécurité conforme à l'état de l'art et aux règles en vigueur dans ce domaine et pour prévenir les agressions éventuelles à partir ou par l'intermédiaire de son/ses Sites (voir annexe 2) ; la nature des données véhiculées ou mises à disposition sur le réseau peut déterminer, à l'initiative et sous la responsabilité du Signataire, un niveau de sécurité particulier qu'il lui appartient de mettre en oeuvre ;

- plus généralement, à se conformer à la présente Charte.

3. Le Signataire de la Charte est informé et accepte expressément que le GIP RENATER procède à des contrôles de la bonne utilisation du réseau RENATER (voir annexe 3) et qu'en cas de manquement à ses obligations telles qu'énoncées à l'article 2 ci-dessus ou, le cas échéant, à la demande de l'autorité de tutelle du ou des Site(s) concerné(s), le GIP RENATER suspende l'accès au réseau RENATER, au niveau national ou international de son ou ses Sites concerné(s).

4. Le Signataire accepte que le GIP RENATER prenne des mesures d'urgence, y inclus la décision de limiter ou d'interrompre temporairement pour le(s) Site(s) concerné(s) l'accès au réseau RENATER au niveau régional, national ou international, pour préserver la sécurité en cas d'incident dont le GIP RENATER aurait connaissance.

   Toutefois, ces mesures :

   - seront accompagnées dans les meilleurs délais d'un dialogue avec le Correspondant de Sécurité du ou des Site(s) concerné(s) ;

   - et ne pourront être mises en oeuvre que dans le cadre d'une procédure approuvée par le conseil d'administration du GIP RENATER et sous réserve de leur faisabilité technique et juridique ;

   - et sur décision des responsables sécurité désignés par les membres fondateurs du GIP RENATER.

   Dans le cas où le(s) Site(s) seraient victime(s) d'actions malveillantes répétées de la part d'un autre Site, sur demande du Signataire du Site ou des Site(s) concerné(s), le GIP RENATER s'engage à mettre en oeuvre les mesures de restriction dans les mêmes termes et conditions que ci-dessus.

5. Le Signataire est informé et accepte expressément que le GIP RENATER modifie la présente Charte notamment pour tenir compte des évolutions législatives à intervenir dans ce domaine ; ces modifications lui seront notifiées périodiquement.

6. Le Signataire de la présente Charte, représentant de la personne morale du ou des Site(s) (nom, prénom, fonction)

reconnaît avoir pris connaissance de la présente Charte de déontologie du Réseau National de télécommunications pour la Technologie, l'Enseignement et la Recherche RENATER, et s'engage à les respecter et les faire respecter par tous ses utilisateurs raccordés au réseau RENATER par l'intermédiaire de la prise RENATER de son Etablissement ou du Site ou des Sites identifié(s) ci-dessous ou de tous les autres sites qui aurai(en)t accès au réseau RENATER dans le cadre d'un contrat établi à cet effet entre le Signataire et le GIP RENATER.

Identification du site ou des sites d'accès[3]
Adresse (s) :

La personne morale désigne comme Correspondant Sécurité, (annexe 2)
Nom, Prénom :
Adresse postale :
Adresse électronique :
Téléphone :
Télécopie :

Le Signataire :
Nom, Prénom :
Titre :
Etablissement :
Date :
Signature :
Cachet :

[3] Le site ou les sites d'accès désigne(nt), celui ou ceux des Site(s) du signataire qui donne(nt) accès à RENATER à l'ensemble des utilisateurs auquel le Signataire donne accès.
A titre d'exemple, dans le cas d'un organisme ayant plusieurs sites qui bénéficient de l'accès à RENATER par l'intermédiaire du réseau interne de l'organisme, seul le site titulaire de la prise d'accès à RENATER doit être mentionné. Par contre, la Charte Déontologique RENATER s'applique à l'ensemble des utilisateurs des sites accédant à RENATER par l'intermédiaire de cet accès. Dans le cas où un des sites précédents hébergerait d'autres entités, l'accord du GIP RENATER doit être obtenu pour qu'elles puissent en bénéficier.

Annexe 1

1. Utilisation à des fins strictement professionnelles du réseau RENATER.

Le réseau RENATER est destiné à véhiculer le trafic engendré par des activités d'enseignement, recherche, développements techniques, transfert de technologies, diffusion d'informations scientifiques, techniques et culturelles, expérimentations de nouveaux services présentant un caractère d'innovation technique.

Les activités d'administration et de gestion des centres de recherche, de développement ou d'enseignement sont assimilées à la recherche ou à l'enseignement.

Les autres activités, notamment vente de services doivent faire l'objet d'un accord préalable et écrit du GIP RENATER, à l'exclusion toutefois des activités commerciales liées à l'enseignement, à la recherche et au développement technique ainsi qu'aux transferts de technologie et à la diffusion d'informations scientifiques, techniques et culturelles.

2. Utilisation rationnelle du réseau RENATER

Pour offrir à l'ensemble des utilisateurs un niveau de qualité optimale, le GIP RENATER limite l'utilisation d'applications consommatrices de ressources de réseau (diffusion de vidéo notamment). Dans ces conditions, la mise en oeuvre d'applications qui engendrent un trafic permanent est soumise à l'accord préalable et écrit du GIP RENATER. Les limitations pourront porter sur des créneaux horaires, ou sur l'utilisation des liaisons nationales ou internationales particulièrement chargées.

Pour ne pas pénaliser le développement et l'expérimentation de ces applications, le GIP RENATER cherchera à en assurer la coordination de mise en oeuvre.

3. Utilisation loyale du réseau RENATER

Le Signataire s'engage à veiller à ce qu'aucun utilisateur sur son/ses Sites ne crée(nt) ou ne génère(nt) sciemment des données ayant pour effet de saturer les liaisons du réseau RENATER ou encore d'épuiser les ressources de ses équipements. En particulier, les automates à base de requêtes ICMP sur les routeurs du réseau RENATER sont interdits, sauf accord préalable et écrit du GIP RENATER.

4. Licité des données véhiculées sur le réseau RENATER

Les données véhiculées et mises à disposition sur le réseau à l'initiative des utilisateurs du réseau RENATER doivent être licites. A ce titre, les utilisateurs doivent respecter l'ensemble des dispositions légales, notamment :

- le Code de la Propriété Intellectuelle qui fait interdiction d'utiliser, de reproduire et plus généralement d'exploiter des oeuvres protégées par le droit d'auteur, notamment les logiciels, sans l'autorisation de l'auteur ou du titulaire des droits.
- le Nouveau Code Pénal qui sanctionne les atteintes à la personnalité et aux mineurs ainsi que les crimes et délits technologiques.
- la loi du 29 juillet 1881 modifiée, sanctionnant les infractions de presse, notamment la diffamation, le négationnisme, le racisme et les injures.
- la loi sur la cryptologie (loi nº 2004-575 du 21 juin 2004)

Une annexe informative du dispositif légal en vigueur est jointe à la présente Charte en Annexe 4.

5. Fourniture d'accès indirect au réseau RENATER.

Les Sites font l'objet d'une procédure d'agrément (voir feuillet d'agrément) . L'accès au réseau RENATER est réservé aux seuls utilisateurs des Sites agréés et à eux seuls. A ce titre, tout accès à titre commercial ou non, rémunéré ou non à des tiers non autorisés est interdit sauf accord préalable et écrit du GIP RENATER. Il est également interdit d'offrir des accès par le réseau commuté ou numéris à des individus qui ne sont pas utilisateurs du ou des Sites. Il appartient au Signataire d'identifier et de contrôler les accès. Le Signataire engage à ce titre sa responsabilité propre.

Les accès indirects concernent également la retransmission ou le relais de services d'informations obtenus à travers le réseau RENATER.

Le raccordement au réseau RENATER d'autres réseaux, nationaux, étrangers, internationaux, ou prestataires de services commerciaux, par l'intermédiaire d'un Site agréé est sujet à l'accord préalable du GIP RENATER. Il devra faire l'objet d'une procédure d'agrément.

Toutefois lorsqu'un Site fait partie d'une communauté ou d'une entreprise (centre de recherche industriel au sein d'une entreprise, école dépendant d'une chambre de commerce, service d'enseignement et laboratoire de recherche universitaires au sein d'un centre hospitalier universitaire....), et que son réseau est connecté à des réseaux de cette communauté ou de cette entreprise, le Signataire a pour seules obligations :

- de ne pas donner accès au réseau RENATER aux utilisateurs des réseaux de cette communauté ou de cette entreprise ;
- d'informer le responsable de ces réseaux de la teneur de la présente Charte qui implique que les utilisateurs de ces réseaux ne peuvent accéder à Renater;
- de prendre toutes mesures d'isolement ou de filtrage de ces réseaux, s'ils sont directement ou indirectement à l'origine d'incidents sur le réseau RENATER.

Annexe 2
Sécurité

Le Signataire, seul responsable de la sécurité de ses équipements, s'engage à mettre en oeuvre une politique de sécurité d'un niveau conforme à l'état de l'art et aux règles en vigueur dans ce domaine.

A ce titre, il appartient au Signataire de mettre en oeuvre les ressources techniques et humaines requises pour protéger son ou ses Site(s) et pour éviter les agressions contre d'autres sites connectés au réseau RENATER ou à d'autres réseaux ou encore contre le réseau RENATER à partir ou par l'intermédiaire de son ou de ses Site(s). Des informations sur ce sujet sont accessibles sur le site Web de Renater. Il est demandé au Signataire de veiller tout particulièrement aux accès à leur(s) Site(s) par le réseau commuté ou par le réseau Numéris.

Par ailleurs, il appartient au Signataire de désigner une personne dénommée « Correspondant Sécurité » et de faire assurer la formation et l'information des utilisateurs du ou de ses Sites.

Le Correspondant Sécurité :

Pour ce qui concerne les événements liés à la sécurité, le Correspondant Sécurité doit disposer de tous les pouvoirs opérationnels nécessaires pour intervenir efficacement et dans les meilleurs délais, en cas d'incident de sécurité, notamment à la demande du GIP RENATER, tant au niveau de la connexion du ou des Sites agréés du Signataire que sur les éventuelles connexions directes vers d'autres sites.

Lorsqu'un incident de sécurité se produit sur le(s) Site(s) du Signataire, de nature à impliquer un ou plusieurs autres Sites et/ou le réseau RENATER, le Correspondant Sécurité du Site concerné doit informer le GIP RENATER dans les meilleurs délais, et, au besoin, dans la mesure de son possible, prévenir les autres sites et apporter son concours à la solution de l'incident.

Le devoir d'information et de formation des Utilisateurs.

Le Signataire s'engage à informer les utilisateurs, notamment les administrateurs de systèmes informatiques, de son/ses Site(s) de la teneur de la présente Charte, à s'assurer qu'ils en ont effectivement pris connaissance, et à demander aux directions des autres sites ayant accès au réseau RENATER via son propre Site de faire la même démarche. A cet effet, il est conseillé de faire signer par les utilisateurs une déclaration indiquant qu'ils en ont pris connaissance.

Par ailleurs, le Signataire s'engage à mettre en oeuvre les actions de formation nécessaires.

Annexe 3

Le Signataire accepte que le GIP RENATER puisse vérifier la bonne utilisation par les utilisateurs de son/ses Site(s) du réseau RENATER. A cet effet, il accepte que le GIP RENATER ait accès, notamment auprès des opérateurs concernés, aux informations d'administration de réseau (telles que des données de volumétrie, d'incidents, etc...) concernant son/ses Site(s). Elles seront considérées par le GIP RENATER comme confidentielles, et seuls des bilans de synthèse globaux pourront être rendus publics en dehors de l'accord explicite du Signataire ou, le cas échéant, de son autorité de tutelle.

Le Signataire reconnaît que les conditions de confidentialité de ces informations figurant éventuellement dans le (ou les) contrat(s) qu'il a signé(s) avec l'opérateur lui donnant directement ou indirectement accès à RENATER ne sont pas opposables, ni par lui ni par l'opérateur, à la communication d'informations définie ci-dessus.

Annexe 4

Liste informative des infractions susceptibles d'être commises

1. Infractions prévues par le Nouveau Code pénal

1.1. Crimes et délits contre les personnes

- **Atteintes à la personnalité:**

(Respect de la vie privée art. 9 du code civil)

- Atteintes à la vie privée (art. 226-1 al. 2 ; 226-2 al. 2, art.432-9 modifié par la loi nº 2004-669 du 9 juillet 2004)
- Atteintes à la représentation de la personne (art. 226-8)
- Dénonciation calomnieuse (art. 226-10)
- Atteinte au secret professionnel (art. 226-13)
- Atteintes aux droits de la personne résultant des fichiers ou des traitements informatiques (art. 226-16 à 226-24, issus de la loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés

- **Atteintes aux mineurs**: (art. 227-23 ; 227-24 et 227-28).

Loi 2004-575 du 21 juin 2004 (LCEN)

1.2. Crimes et délits contre les biens

- Escroquerie (art. 313-1 et suite)
- Atteintes aux systèmes de traitement automatisé de données (art. 323-1 à 323-7 modifiés par la loi nº 2004-575 du 21 juin 2004).

1.3 Cryptologie

- Art. 132-79 **(**inséré par loi nº 2004-575 du 21 juin 2004 art. 37**)**

2. Infractions de presse (loi 29 juillet 1881, modifiée)

- Provocation aux crimes et délits (art.23 et 24)
- Apologie des crimes contre l'humanité (art. 24)
- Apologie et provocation au terrorisme (art. 24)
- Provocation à la haine raciale (art. 24)
- « Négationnisme »: contestation des crimes contre l'humanité (art. 24 bis)
- Diffamation (art. 30.31 et 32)
- Injure (art. 33)

3. Infraction au Code de la propriété intellectuelle

- Contrefaçon d'une oeuvre de l'esprit (y compris d'un logiciel) (art. 335-2 modifié par la loi nº 2004-204 du 9 mars 2004, art. 34 - et art. 335-3)
- Contrefaçon d'un dessin ou d'un modèle (art. L521-4 modifiée par la loi nº 2004-204 du 9 mars 2004, art. 34)
- Contrefaçon de marque (art. L716-9 - modifié par la loi nº 2004-204 du 9 mars 2004, art. 34 -et suivants)

4. Participation à la tenue d'une maison de jeux de hasard (« cyber-casino »)

- Art.1 de la loi du 12 juillet 1983, modifié par la loi du 16 décembre 1992

C Charte CentraleSupélec

Annexe 2
au Règlement Intérieur

CHARTE INFORMATIQUE
CentraleSupélec

Utilisation des technologies de l'information et de la communication

Article 1er - Textes applicables et définitions

Il est rappelé que toute personne sur le sol français doit respecter l'ensemble de la législation applicable, notamment dans le domaine de la sécurité informatique, et tout particulièrement :

- la loi n° 78-17 du 6 janvier 1978 dite « informatique et libertés » ;
- la législation relative aux atteintes aux systèmes de traitement automatisé de données (article 323-1 à 323-7 du Code pénal) ;
- les dispositions du Code du travail ;
- l'article L. 241-1 du Code de la Sécurité Intérieure relatif au secret des correspondances ;
- la législation relative à la propriété intellectuelle ;
- la loi n° 94-665 du 04 août 1994 relative à l'emploi de la langue française ;
- la législation applicable en matière de cryptologie ;
- les législations sur l'audiovisuel et les télécommunications en ce qui concerne les grands principes applicables aux communications publiques et privées.

Dans la suite du document :

- le terme « ressource informatique » recouvre tous les moyens informatiques (e.g. ordinateur, tablette, smartphone, connectivité au réseau de l'Ecole ou aux réseaux Internet et Renater, logiciels, programmes, …) mis à disposition par CentraleSupélec ;
- le terme « ressource de téléphonie » recouvre tous les moyens de téléphonie (e.g. téléphone fixe ou mobile) mis à disposition par CentraleSupélec ;
- le terme « outils de partage et de transmission d'informations » recouvre tous les moyens informatiques de diffusion d'informations (e.g. messagerie, forum de discussion, cloud, base d'informations, logiciels collaboratifs, réseau social, …) ;
- le terme « utilisateur » recouvre toute personne, quel que soit son statut (e.g. personnel, collaborateur, prestataire, vacataire, élève, visiteur, …) ayant accès à au moins une ressource informatique ou de téléphonie ;
- le terme « compte » recouvre l'identifiant et le mot de passe nécessaires pour s'authentifier en vue de l'accès à des ressources informatiques.

Article 2 - Principaux objectifs

2.1) Afin de permettre aux utilisateurs d'exercer leur activité dans les meilleures conditions, CentraleSupélec s'est doté de ressources informatiques, chaque utilisateur dont l'activité le requiert disposant pour l'essentiel :

- de matériels reliés au réseau Internet, tels qu'ordinateurs, tablettes ou téléphones mobiles (encore appelés smartphones) ;
- de logiciels de bureautique ;
- d'une messagerie.

Certains utilisateurs disposent d'un poste portable ou d'une tablette pour travailler/se connecter à distance.

Les moyens informatiques de CentraleSupélec sont, en pratique, administrés par la Direction des Systèmes d'Informations (DSI) et par des structures correspondantes sur les campus de Metz et de Rennes.

2.2) Compte tenu de l'importance de ces moyens, CentraleSupélec a souhaité insérer en annexe de son règlement intérieur, les présentes dispositions, et ce afin de permettre aux utilisateurs de :

- prendre conscience des menaces pesant sur la sécurité du système d'information de l'Ecole ;
- mesurer les risques, notamment en terme de responsabilité qui peuvent être liés à l'utilisation incorrecte des technologies de l'information et de la communication ;
- connaître les moyens mis en œuvre par l'Ecole pour préserver l'intégrité du réseau et des données qui lui appartiennent tout en respectant la vie privée d'autrui ;
- adopter un comportement conforme aux attentes de CentraleSupélec, le non-respect des directives émises étant notamment susceptible de conduire à la mise en cause, le cas échéant, de la responsabilité disciplinaire de l'utilisateur.

Tout utilisateur doit se conformer à la présente charte et s'engage personnellement à la respecter. Cette charte est conforme aux recommandations de la charte individuelle de bon usage RENATER.

Article 3 - Conditions d'accès aux ressources informatiques

3.1) Afin d'accéder aux ressources informatiques, chaque utilisateur se voit confier un ou plusieurs comptes, ceux-ci étant composés de :

- un nom d'utilisateur attribué personnellement à chacun par la DSI ;
- un mot de passe choisi par chaque utilisateur et composé individuellement en respectant les critères prescrits par la DSI.

A des fins de sécurité la DSI pourra prévoir – sur une base régulière ou non – les conditions de changement impératif du mot de passe par l'utilisateur.

3.2) Chaque utilisateur est personnellement responsable de son compte, sa divulgation à d'autres utilisateurs ou à des tiers non autorisés étant prohibée.

Par exception à ce principe et dans le seul cas où la délégation de droits est inexistante dans les outils logiciels, il est toléré qu'un utilisateur puisse se voir confier par un autre un droit d'accès à son matériel ou à sa messagerie professionnelle ou à des applications métiers, et ce afin d'assurer le bon fonctionnement ou la continuité du service (par exemple, en cas d'absence ou de congé…).

Ce droit d'accès – qui se traduit par une transmission du compte – est soumis aux conditions suivantes :

- il ne peut intervenir qu'entre personnels de CentraleSupélec, toute divulgation du compte à un tiers ou à un stagiaire étant prohibée ;
- il donnera lieu à la rédaction d'une autorisation écrite et temporaire ;
- le personnel habilité à avoir accès à l'ordinateur ou à la messagerie d'un autre ne pourra, en aucun cas, prendre connaissance de fichiers ou messages identifiés comme personnels ;
- le personnel ayant temporairement confié son compte à un autre devra – postérieurement à l'exercice de ce droit d'accès – modifier son mot de passe.

3.3) L'utilisation des ressources informatiques de CentraleSupélec et la connexion d'un équipement sur le réseau sont soumises à autorisation de la DSI. Il est interdit de connecter au réseau filaire un équipement non référencé par CentraleSupélec sauf accord explicite de la DSI. Ces autorisations sont strictement personnelles et ne peuvent en aucun cas être cédées, même temporairement à un tiers.

Toute autorisation prend fin lors de la cessation de l'activité professionnelle qui l'a justifiée.

3.4) CentraleSupélec pourra en outre prévoir des restrictions d'accès spécifiques à son organisation.

3.5) « Eduroam » (i.e. Education Roaming) est un service d'accès international développé par la communauté internationale de la Recherche et de l'Enseignement. Un accès WiFi Eduroam, disponible pour tous les utilisateurs, permet une connexion depuis les différents sites de CentraleSupélec mais également depuis la plupart des universités et écoles.

3.6) Chaque utilisateur est responsable de la sauvegarde et de la protection de ses données. Les données peuvent être copiées sur des ressources mises à disposition par l'école et régulièrement sauvegardées.

3.7) Un accès WiFi est mis à la disposition des visiteurs de passage. Il reviendra au personnel de CentraleSupélec accueillant le visiteur d'effectuer les démarches nécessaires.

Article 4 - Utilisation des ressources informatiques et de téléphonie

4.1) Principes généraux

Les ressources informatiques et de téléphonie mises à disposition de chaque utilisateur devront être utilisées pour l'essentiel pour les seuls besoins de l'exercice de l'activité professionnelle.

Sans que cette liste soit limitative, chaque utilisateur s'engage ainsi à :

- ne pas porter atteinte à la sécurité des ressources informatiques ;

- respecter les conditions des licences d'utilisation des logiciels ;
- ne pas tenter d'en perturber le fonctionnement ;
- ne pas modifier la configuration de base des ressources informatiques ;
- ne pas masquer son identité et/ou usurper l'identité d'un tiers ;
- respecter et appliquer les mesures de sécurité qui lui seront transmises par la DSI ;
- assurer la protection de ses informations en respectant la confidentialité afférente ;
- protéger ses données en utilisant les différents moyens de sauvegarde individuels ou mis à sa disposition par l'école ;
- ne pas mettre à la disposition d'utilisateurs non autorisés un accès aux systèmes ou aux réseaux à travers des moyens dont il a l'usage ;
- ne pas tenter de lire, modifier, copier ou détruire des données sans l'accord de leur propriétaire, quand bien même celui-ci ne les auraient pas explicitement protégées ;
- préserver la confidentialité de l'accès aux informations et documents conservés sur les systèmes informatiques de l'Ecole ;
- ne pas prendre connaissance d'informations et/ou de documents transitant sur le réseau sans l'accord explicite de la DSI ;
- privilégier une connexion WiFi de confiance à une connexion au réseau mobile, pour minimiser les coûts afférents de transfert de données, notamment lors de déplacements à l'étranger.

L'utilisation des ressources informatiques et de téléphonie à des fins pénalement répréhensibles ou pour des usages pouvant nuire aux intérêts de CentraleSupélec, à son image ou à sa réputation, est interdite.

Sans que cette liste soit limitative, chaque utilisateur s'engage ainsi, à l'aide de ressources informatiques ou de téléphonie de CentraleSupélec, à :

- ne pas consulter volontairement, produire, copier, télécharger, diffuser des informations dont le contenu présente un caractère pédophile, négationniste ou portant atteinte à la dignité humaine ;
- ne pas les utiliser à des fins politiques, religieuses, pornographiques ou contraire aux règles de déontologie (*terme pour désigner l'ensemble de règles régissant une profession*) /d'éthique professionnelle ;
- ne pas participer à des jeux en ligne et/ou commettre tout agissement visant à obtenir des profits ou gains personnels ;

- ne pas commettre d'action susceptible de porter atteinte à la sûreté et sécurité du personnel et des élèves de CentraleSupélec.

4.2) Respect de la vie privée

Conformément aux recommandations de la CNIL, CentraleSupélec tolère un usage raisonnable de ses ressources informatiques et de téléphonie dans le cadre des nécessités de la vie courante et familiale ; de manière générale, un tel usage ne doit pas affecter la sécurité des réseaux ou la productivité.

Pour les ressources informatiques et les outils de partage et de transmission d'informations :

- les fichiers et messages stockés sur les matériels de l'utilisateur sont réputés avoir un caractère professionnel sauf s'ils sont identifiés comme étant personnels ;
- pour être identifiés comme personnels, les fichiers et messages doivent soit contenir dans leur nom ou objet le mot personnel et/ou privé, soit être rangés dans un dossier dont le nom commence par le mot personnel ou privé ;
- l'employeur peut, hors de la présence de l'agent et pour des nécessités de service, consulter les fichiers et messages professionnels ;
- en cas de risque ou événement particulier, l'employeur peut avoir accès aux fichiers et messages identifiés comme personnels de l'agent, et vérifier notamment que ceux-ci n'enfreignent ni les textes de lois ni les dispositions de la présente Charte, cette vérification devant être opérée sous réserve que l'agent concerné soit présent ou qu'il ait été dûment appelé (un délai de prévenance d'un jour ouvré devant être respecté) ;
- en cas de risque ou événement particulier, l'employeur peut vérifier que les fichiers et messages identifiés comme personnels ne sont pas à l'origine du problème identifié.

4.3) Signalement

Chaque utilisateur doit signaler toute tentative de violation de son compte, et de façon générale, toute anomalie qu'il peut constater à la DSI qui, le cas échéant, transmettra les informations utiles à la Direction de CentraleSupélec.

4.4) Téléchargements/ Installations de logiciels

Le téléchargement et le stockage de vidéos et/ou musique à des fins personnelles sur les ressources informatiques communes sont prohibés.

L'installation de logiciels sur les ressources informatiques est habituellement réalisée par la DSI ou par une personne habilitée.

Pour raisons de service, un utilisateur pourra obtenir auprès de la DSI les privilèges d'administration de son poste de travail après accord de son responsable d'entité.

Un utilisateur pourra être tenu responsable des conséquences s'il installe par lui-même un logiciel non approuvé par la DSI.

4.5) Départ définitif de l'utilisateur

Tout utilisateur qui quitte CentraleSupélec doit :

- supprimer des ressources informatiques de l'Ecole tout contenu (e.g. message, fichier, …) pouvant présenter un caractère personnel ;
- transmettre à son entité, avant son départ, toutes les données professionnelles qui pourraient être utiles en portant une attention particulière aux données créées sous son compte et partagées avec d'autres personnes. Données pour lesquelles il sera nécessaire de transférer la propriété avant suppression du compte ;
- rendre toutes les ressources informatiques et de téléphonie qui lui ont été confiées.

D'une manière générale, toutes dispositions doivent être prises par l'utilisateur concernant la partie "privée" de ses ressources informatiques et des outils de partage et de transmission d'informations, de telle sorte qu'il ne reste plus que les informations professionnelles utiles dans les ressources informatiques locales ou distantes de CentraleSupélec.

Article 5 - Modalités d'utilisation des outils de partage et de transmission d'informations

5.1) La messagerie est un outil qui est, par principe et pour l'essentiel, destiné à un usage professionnel.

5.2) CentraleSupélec reconnaît qu'une utilisation ponctuelle et modérée de la messagerie à laquelle les utilisateurs ont accès peut être tolérée à des fins personnelles, à la condition de :

- ne pas porter atteinte à la sécurité du réseau informatique de l'Ecole ;
- intervenir pour les stricts besoins de la vie courante ou familiale ;
- ne pas porter atteinte aux performances du réseau de l'école, ceci imposant que les pièces jointes aux messages personnels ne dépassent pas 10 méga octets ;
- le transfert de documents supérieurs à 10 méga octets ne doit pas se faire, sauf cas particulier, via la messagerie, mais en utilisant les outils spécifiques proposés par la DSI.

5.3) L'utilisation des listes de diffusion internes à CentraleSupélec est réservé à un usage professionnel et doit se faire selon les règles édictées par la DSI, disponibles auprès de la DSI.

5.4) L'utilisation de tout autre outil de partage et de transmission d'informations est réservé à un usage professionnel.

Article 6 - Obligations de l'utilisateur des outils de partage et de transmission d'informations

6.1) Les utilisateurs veilleront tout particulièrement à ce que les messages envoyés ou informations partagées ne portent pas atteinte à l'image ou aux intérêts de l'Ecole

A ce titre, et pour quelque motif que ce soit, les messages adressés ou informations partagées par l'utilisateur ne devront pas :

- comporter des dénigrements et/ou des propos diffamatoires à l'égard de l'Ecole, de ses concurrents ou de quiconque ;
- porter atteinte aux intérêts directs ou indirects de l'Ecole et/ou à son image ;
- comporter des éléments offensants et/ou discriminatoires liés notamment à la race, l'origine, le sexe, la religion, les opinions politiques, l'âge ou le handicap ;
- comporter des allusions, propos, images ou vidéos de nature sexuelle, pornographiques, pédophiles, liés à un harcèlement sexuel ou induisant des comportements dégradants ;
- procéder à l'envoi de documents en masse, participer à des chaînes ou encore effectuer un renvoi permanent de ses messages entrants vers une autre adresse de messagerie.

6.2) Tout message reçu par l'utilisateur à titre privé et ne respectant pas les principes ci-dessus devra impérativement être détruit. S'il s'agit d'un message à caractère professionnel, l'utilisateur pourra en avertir la DSI en fonction de l'importance de l'infraction.

6.3) Les espaces de discussion en ligne sont des espaces de liberté de parole, régis, comme dans la vie réelle, par des obligations légales. L'internaute est responsable de ce qu'il dit ou diffuse sur ces réseaux.

La frontière étant très ténue entre « Identité personnelle » et « Identité professionnelle », l'utilisateur devra porter attention à l'usage qui pourrait être fait des informations qu'il publie sur les réseaux sociaux.

Article 7 - Modalités d'utilisation du réseau

7.1) L'accès au réseau Intranet/Internet est prévu au sein de CentraleSupélec pour l'accomplissement de l'activité professionnelle.

7.2) A titre de tolérance, un usage privé de l'Internet pourra être accepté par CentraleSupélec, dès lors que :

- les sites consultés ne sont pas contraires à l'ordre public ou aux bonnes mœurs ;
- cet usage ne porte pas atteinte au bon fonctionnement du système d'information ;
- la durée de consultation est raisonnable et n'interfère pas avec les obligations professionnelles ;

- cet usage personnel d'Internet n'induit aucune charge financière directe ou indirecte pour l'Ecole.

Article 8 - Obligations de l'utilisateur du réseau

Dans le cadre de l'utilisation du réseau Internet, les utilisateurs veilleront à adopter un comportement ne pouvant porter atteinte à l'image ou aux intérêts de CentraleSupélec.

Sans que cette liste soit limitative, sont notamment interdits :

- la diffusion de son compte sur tout site et/ou messagerie externe à CentraleSupélec, notamment afin de mettre en place une relève automatique de la boîte à lettres professionnelle de CentraleSupélec par un autre fournisseur de services de messageries ;
- l'usurpation de l'identité (par exemple du compte) d'une personne ;
- l'utilisation des ressources informatiques de l'Ecole dans le cadre de l'exercice d'une activité commerciale personnelle ;
- toute action susceptible de mettre en cause la sécurité de l'Ecole ou de porter atteinte à sa réputation ;
- les tentatives de violation d'accès ou l'accès non autorisé au système informatique de l'Ecole ou de toute autre organisation ;
- les connexions (ou tentatives de connexions) sur un serveur autrement que par les dispositions prévues par ce serveur et/ou sans y être autorisé par les responsables habilités ;
- toute action, de quelque nature que ce soit, mettant sciemment en péril la sécurité ou le bon fonctionnement des serveurs de l'Ecole ;
- l'utilisation des ressources informatiques ou du réseau pour proposer ou rendre accessible à des tiers des données et informations confidentielles ou contraires à la législation en vigueur ;
- tout non-respect des lois et notamment celles relatives aux publications à caractère illicite, injurieux, raciste, pornographique, diffamatoire, tout propos discriminatoire par exemple liés à la race, l'origine nationale, le sexe, la religion, les opinions politiques, les origines sociales, l'âge ou le handicap.

L'utilisateur veillera tout particulièrement au moyen de ressources informatiques de l'Ecole à éviter de :

- se connecter via des réseaux publics, notamment WiFi, tels que gares, hôtels, restaurants, bars, squares, …
- d'ouvrir des pièces jointes en provenance d'un utilisateur inconnu.

Pour préserver la qualité de ses réseaux, notamment sans fil, l'Ecole mettra en place les mesures adéquates pour détecter et écarter les perturbateurs (e.g. smartphones en mode diffusion de point d'accès WiFi).

Article 9 - Examen des ressources informatiques et de téléphonie

9.1) Rappel Général

Pour des nécessités de maintenance et de gestion technique, de contrôle à des fins statistiques, de traçabilité, d'optimisation, de sécurité, ou afin d'assurer le respect des dispositions prévues par le présent titre, l'utilisation des ressources matérielles ou logicielles ainsi que les échanges via le réseau peuvent, sous le contrôle de CentraleSupélec, être analysés et contrôlés dans le respect de la législation applicable et notamment de la loi « informatique et libertés ».

CentraleSupélec s'engage, dans le cadre de ses contrôles, à :

- ne pas porter atteinte aux droits qu'a chacun au respect de sa vie privée, conformément aux dispositions des articles 8 de la Convention Européenne des Droits de l'Homme et l'article 9 du Code Civil ;
- ne mettre en place ces contrôles que conformément au principe de proportionnalité prévu à l'article L. 1121-1 du Code du Travail.

9.2) Contrôle de l'utilisation de la téléphonie

Afin d'assurer le respect des dispositions prévues par la présente charte, CentraleSupélec pourra mettre en œuvre des moyens de contrôles adaptés.

CentraleSupélec se réserve ainsi le droit de contrôler le nombre, les destinataires et la durée des appels envoyés et reçus par les utilisateurs.

De la même façon, l'usage de la transmission de données ou de la consultation Internet via des abonnements professionnels mis à disposition par CentraleSupélec pourra faire l'objet d'analyses.

Ces dispositions ne concernent pas les postes téléphoniques mis à la disposition des associations ou des représentants du personnel dans l'exercice de leurs activités.

9.3) Contrôle de l'utilisation de la messagerie électronique

Afin d'assurer le respect des dispositions prévues par la présente charte, CentraleSupélec pourra mettre en œuvre des moyens de contrôles adaptés.

CentraleSupélec se réserve ainsi le droit de contrôler le nombre, les adresses et la taille des messages envoyés et reçus par les utilisateurs.

CentraleSupélec, notamment en cas d'absence de l'agent pour quelque motif que ce soit, est en droit de prendre connaissance du contenu des messages autres que ceux identifiés comme personnels

conformément à l'article 4.2, ou s'ils ne sont pas identifiés comme échangés dans le cadre d'une fonction de représentant du personnel.

9.4) Contrôle de la consultation des sites Internet et de l'usage des outils de partage et de transmission d'informations

Afin d'assurer le respect des dispositions prévues par la présente charte, CentraleSupélec se réserve le droit de consulter l'ensemble des traces informatiques qui résultent de la consultation des sites internet ou de l'usage des outils de partage et de transmission d'informations, et qui permettent notamment de déterminer les heures et durées de consultation, ainsi que les sites consultés.

CentraleSupélec s'engage à ne pas utiliser ces traces informatiques à d'autres fins que celles qui sont strictement liées au contrôle de l'utilisation des ressources informatiques conformément à cette charte.

Dans tous les cas, CentraleSupélec s'engage à ne pas utiliser ces traces informatiques au-delà d'un délai de 3 mois. Les traces sont néanmoins conservées conformément aux pratiques conseillées pour répondre aux demandes des services de Justice.

9.5) Modalités de contrôle

CentraleSupélec se réserve le droit de procéder à des contrôles de l'utilisation des ressources informatiques, ces contrôles pouvant prendre en compte :

- la fréquence et le volume des documents émis ou reçus ;
- le bon respect des conditions d'utilisation des ressources informatiques ;
- la nature des sites visités.

Article 10 - Administrateur réseau

Le ou les administrateurs de réseaux de CentraleSupélec à savoir les personnels et les prestataires dûment mandatés par la DSI sont :

- investis de droits étendus pour mener à bien la tâche qui leur est assignée d'assurer et de veiller au bon fonctionnement des systèmes ;
- tenus à l'obligation de secret et de confidentialité eu égard aux informations dont ils pourraient avoir connaissance dans le cadre de leur activité ;
- tenus d'informer leur hiérarchie des incidents ou dysfonctionnements que les utilisateurs peuvent constater ou provoquer eu égard aux systèmes auxquels ils ont accès.

Article 11 – Manquements

Les non-respects de la charte informatique peuvent entraîner l'application de sanctions disciplinaires, sans préjudice des autres poursuites envisageables (mise en cause de la responsabilité civile, mise en cause de la responsabilité pénale).

Article 12 - Respect des compétences de la CNIL

Conformément à la législation en vigueur, les moyens de contrôle visés par cette charte respectent les principes définis par la Commission Nationale Informatique et Libertés et ont été soumis au Correspondant Informatique et Liberté (CIL) de CentraleSupélec.

Les utilisateurs sont par ailleurs invités à demander conseil au CIL de CentraleSupélec pour les éventuelles formalités à accomplir s'ils constituent des fichiers soumis aux dispositions de la loi « informatique et libertés ».

Article 13 - Formalités - Entrée en vigueur

13.1) Compte tenu de la consultation des représentants du personnel opérée le 04 mai 2016, la présente charte entrera en vigueur à compter du 16 juin 2016.

13.2) La présente charte annule et remplace, dès son entrée en vigueur, les termes des précédentes Chartes ou tout autre pratique – écrite ou non écrite – appliquées au sein de l'Ecole Centrale Paris et de Supélec.

La présente charte est annexée au règlement intérieur de CentraleSupélec. Elle est mise en ligne sur le site intranet de l'école.