CHARTE NUMERIQUE
CentraleSupélec

Utilisation des technologies de l'information et de la communication

Table des matières

Préambule

La présente charte a pour objet de fixer les règles d'usage des moyens numériques de CentraleSupélec. Le numérique se définit comme l'usage des moyens informatiques (matérie l, logiciel et réseaux).

Ces règles ont pour but de contribuer à la sécurité du système d'information et de garantir l'intégrité, la disponibilité et la confidentialité des données qui y sont hébergée tout en définissant l'usage du numérique au sein de notre école.

Article 1er – Principaux textes de références 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 :

- Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 (RGPD) et Loi 78-17 du 6 janvier 1978 (dite « informatique et libertés ») modifiée relative à l'informatique, aux fichiers et aux libertés
  - traitement automatisé ou non des données à caractère personnel
  - commission nationale de l'informatique et des libertés (CNIL)
  - obligations des responsables de traitements et droits des personnes
  - délégué à la protection des données (DPO)
- Loi n° 83-634 du 13 juillet 1983 portant droits et obligations des fonctionnaires
  - obligations de secret professionnel, de réserve et de discrétion professionnelle
  - devoir de moralité, de probité et de neutralité
- Loi n°84-16 du 11 janvier 1984 portant dispositions statutaires relatives à la fonction publique de l'Etat et Décret n° 86-83 du 17 janvier 1986 relatif aux dispositions générales applicables aux agents contractuels de l'Etat
  - sanctions applicables aux personnels ingénieurs, administratifs, techniques et de service titulaires
  - sanctions applicables aux agents administratifs contractuels
- Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique
  - obligation des hébergeurs de contenus de lutter contre les infractions par la mise en place d'un dispositif de signalement (information des autorités publiques des activités illicites)
  - obligation des hébergeurs de contenus de garantir la sécurité du stockage des données et de leur transmission
- Code de l'éducation
  - sanctions applicables aux usagers de l'enseignement supérieur
  - sanctions applicables aux enseignants-chercheurs et aux membres des corps des personnels enseignants de l'enseignement supérieur
  - sanctions applicables aux autres enseignants
- Code de la propriété intellectuelle
  - protection des œuvres de l'esprit
  - protection des logiciels et des bases de données
  - protection des marques
  - l'exception pédagogique (article L122-5 3° a et e)
- Code pénal
  - Le secret professionnel (articles 226-13 et 226-14)
  - le secret des correspondances (articles 226-15 et 432-9)
  - atteintes aux systèmes de traitement automatisé de données (article 323-1 à 323-7)
- Autres
  - 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.
- Arrêté du 4 novembre 2014 relatif aux conditions générales d'utilisation, par les organisations syndicales des technologies de l'information et de la communication dans la fonction publique de l'état

Dans la suite du document :

- les termes « ressource informatique » et « moyens numériques », recouvrent tous les moyens informatiques (ex. ordinateur, tablette, smartphone, connectivité au réseau de l'Ecole ou aux réseaux Internet et Renater, logiciels, programmes, …) mis à disposition par CentraleSupélec. En d'autres termes, les moyens numériques ou ressource informatique représentent l'ensemble des logiciels et matériels, outils informatiques et services numériques, que CentraleSupélec met à disposition de ses utilisateurs. ;
- le terme « ressource de téléphonie » recouvre tous les moyens de téléphonie (ex. 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 (ex. messagerie, forum de discussion, cloud, base d'informations, logiciels collaboratifs, réseau social, …) ;
- le terme « utilisateur » recouvre toute personne ayant obtenu l'autorisation d'accéder à au moins une ressource informatique ou de téléphonie de CentraleSupélec, quel que soit son statut (ex. personnel, collaborateur, prestataire, vacataire, élève, visiteur, …). Cet accès se réalise au moyen d'un compte nominatif créé dans le système d'information au profit de l'utilisateur, pour la durée de son activité à CentraleSupélec. Appelé « compte informatique », il est formé d'un identifiant - ou « login » - propre à un utilisateur et attribué lors de son arrivée à CentraleSupélec, et d'un mot de passe choisi par l'utilisateur. Le cycle de vie des comptes informatiques est régi par un ensemble de règles qui garantissent l'expiration du compte au départ de l'utilisateur. CentraleSupélec ne reconnaît pas un droit général au maintien d'un accès au système d'information et, par voie de conséquence au maintien du compte informatique, après le départ de l'utilisateur.
- le terme « compte » recouvre l'identifiant et le mot de passe nécessaires pour s'authentifier en vue de l'accès à des ressources informatiques.

La présente charte définit les règles d'utilisation des ressources informatiques de l'établissement public CentraleSupélec, en conformité avec la législation en vigueur et la charte déontologique[1] du Réseau National de télécommunications pour la Technologie, l'Enseignement et la Recherche (RENATER), afin de permettre le fonctionnement normal des systèmes d'information sous-jacents.

Les dispositions de la présente charte s'appliquent également aux utilisateurs membres du personnel de CentraleSupélec autorisés à exercer leurs missions dans les conditions de télétravail ou de mobilité en France ou à l'étranger.

Les utilisateurs ayant des fonctions d'administrateur des moyens numériques utilisant un compte générique ou nominatif seront également soumis à cette charte (voir article 8 qui précise leurs droits et obligations particulières).

Les usages relevant de l'activité des organisations syndicales sont régis par un document spécifique qui viendra compléter la présente charte.

Enfin, un guide d'utilisateur des outils numériques et une charte sur la qualité de vie numérique pourront venir compléter les règles énoncés dans cette présente charte.

[1] https://www.renater.fr/telechargement%2C1392

Article 2 - Conditions d'utilisation des systèmes d'information et moyens numériques

2.1 Utilisation professionnelle / privée

CentraleSupélec met à la disposition de ses utilisateurs un ensemble d'outils et de services numériques à des fins professionnelles.

Au sens de la présente charte, l'usage des moyens numériques présente un caractère professionnel lorsqu'il intervient :

- dans le cadre des missions confiées par CentraleSupélec, pour les utilisateurs membres de son personnel : enseignants-chercheurs, enseignants, doctorants, post-doctorants, personnels administratifs, techniques, sociaux et de santé, mais également ses prestataires et partenaires ;
- dans le cadre des activités pédagogiques, pour ses utilisateurs étudiants.

Par opposition, l'utilisation à des fins privées doit être non lucrative et limitée, tant dans la fréquence que dans la durée. Elle ne doit nuire ni à la qualité du travail de l'utilisateur, ni au temps qu'il y consacre, ni au bon fonctionnement du service.

Cette utilisation à des fins privées doit se faire dans le strict respect des principes de sécurité exposés à l'article 3 de la présente charte. Son impact doit demeurer négligeable pour CentraleSupélec : elle ne doit en conséquence entraîner ni surcoût pour l'établissement, ni augmentation des risques pour la sécurité des données et des équipements professionnels.

Toute information est réputée professionnelle à l'exclusion des données explicitement désignées par l'utilisateur comme relevant de sa vie privée. Il appartient à l'utilisateur de procéder au stockage de ses données à caractère privé dans un espace prévu à cet effet et identifié sans ambiguïté comme tel. La sauvegarde régulière des données à caractère privé incombera à l'utilisateur.

Ainsi, tout utilisateur manifestera le caractère extra-professionnel d'une partie de ses données en adoptant, exclusivement, le terme « privé » ou « personnel » (ou en anglais : « private », « personal »), pour nommer le dossier de fichiers ou l'objet du message contenant ces informations. Il est à noter que les boites aux lettres liées à une adresse électronique non fournie par l'école seront considérées comme appartenant à l'espace privée.

2.2 Continuité de service : gestion des absences et des départs

Lors d'un départ définitif ou d'une absence ponctuelle ou prolongée, l'utilisateur informe sa hiérarchie des modalités d'accès aux applications et données permettant d'assurer la continuité de service.

Les mesures de conservation des données professionnelles sont définies avec le responsable hiérarchique désigné au sein de CentraleSupélec.

Le responsable hiérarchique d'un utilisateur veillera – en cas de départ de ce dernier – à la suppression des accès ou – en cas de mobilité interne – à la réévaluation des accès et des droits dans les applications professionnelles.

L'utilisateur est responsable de son espace de données à caractère privé. Lors de son départ définitif du service ou de l'établissement, il lui appartient de détruire son espace de données à caractère privé.

Article 3 - Principes de sécurité

3.1 Règles de sécurité applicables

CentraleSupélec met en œuvre les mécanismes de protection appropriés sur les moyens numériques mis à la disposition des utilisateurs.

L'utilisateur est informé que les mots de passe constituent une mesure de sécurité destinée à éviter toute utilisation malveillante ou abusive. Cette mesure ne confère pas un caractère personnel aux outils informatiques protégés.

Les niveaux d'accès ouverts à l'utilisateur sont définis en considération de la mission qui lui est confiée. La sécurité des ressources mises à sa disposition lui impose :

- de respecter les consignes de sécurité, notamment les règles relatives à la gestion des mots de passe ;
- de garder strictement confidentiel(s) son (ou ses) mot(s) de passe et ne pas le(s) dévoiler à un tiers ;
- de respecter la gestion des accès, en particulier ne pas utiliser les noms et mots de passe d'un autre utilisateur, ni chercher à les connaître.

Par ailleurs, la sécurité des ressources mises à la disposition de l'utilisateur nécessite plusieurs précautions :

- de la part de CentraleSupélec :
  - veiller à ce que les ressources sensibles ne soient pas ouvertes à d'autres personnes en cas d'absence sauf dans le cadre des mesures de continuité mises en place par la hiérarchie (voir article 2.2) ;
  - limiter l'accès aux seules ressources pour lesquelles l'utilisateur est expressément habilité ;

- de la part de l'utilisateur :
  - si l'utilisateur ne bénéficie pas d'une autorisation explicite, il doit s'interdire d'accéder ou tenter d'accéder à des ressources du système d'information, même si cet accès est techniquement possible;
  - ne pas connecter directement aux réseaux locaux filaires des matériels non référencés ou non autorisés par CentraleSupélec en dehors des prises réseau OpenZone (dans les salles d'enseignement ou espace de travail partagé) et du Wifi eduroam ou Guest ;
  - ne pas installer, télécharger ou utiliser dans le cadre professionnel ou scolaire, de logiciels ou progiciels sans y être autorisé par la DISI ou le référent informatique de votre laboratoire ;
  - se conformer aux dispositifs mis en place par CentraleSupélec pour lutter contre les virus et les attaques par programmes informatiques (voir https://mycs.centralesupelec.fr/fr/assistance).

3.2 Devoirs de signalement et d'information

CentraleSupélec doit porter à la connaissance de l'utilisateur tout élément susceptible de lui permettre d'apprécier le niveau de risque encouru dans l'utilisation du système d'information.

L'utilisateur doit avertir le support dans les meilleurs délais de tout dysfonctionnement constaté ou de toute anomalie découverte telle une intrusion dans le système d'information. Il signale également à la personne responsable du site toute possibilité d'accès à une ressource qui ne correspond pas à son habilitation.

3.3 Mesures de contrôle de la sécurité

L'utilisateur est informé que :

- pour effectuer la maintenance corrective, curative ou évolutive, CentraleSupélec se réserve la possibilité de réaliser des interventions (le cas échéant à distance) sur les ressources mises à sa disposition ;
- une maintenance à distance sur un poste de travail est précédée d'une information de l'utilisateur ;
- le système d'information peut faire l'objet d'une surveillance et d'un contrôle à des fins statistiques, de traçabilité, d'optimisation, de sécurité ou de détection des abus ;
- Les personnels chargés des opérations de contrôle sont soumis au secret professionnel.

3.4 Protection antivirale

CentraleSupélec a déployé une protection logicielle généralisée non seulement sur les serveurs mais aussi les postes de travail des utilisateurs.
Le but d'un anti-virus est de protéger toutes les machines du parc contre les attaques provoquées par des codes malveillants. Sur chaque poste utilisateur est installé un client anti-virus. Il est interdit par la présente charte de désactiver, d'altérer le fonctionnement ou de désinstaller ce client. Il est aussi interdit d'utiliser d'autres logiciels (anti-virus ou autres) susceptibles d'entraîner un dysfonctionnement de l'anti-virus installé en exécution de la stratégie de sécurité de CentraleSupélec.
Pour plus de détails voir la page https://mycs.centralesupelec.fr/virus-et-spam

L'utilisation à des fins professionnelles d'un matériel autre que celui mis à disposition de l'utilisateur par CentraleSupélec notamment un matériel personnel, doit se faire dans le strict respect des principes de sécurité rappelés dans la présente charte.
Il appartient donc à l'utilisateur qui souhaite accéder aux ressources du système d'information de CentraleSupélec de veiller à la sécurité du matériel qu'il utilise et à son innocuité. Cette obligation incombe également aux membres du personnel qui utilisent un matériel informatique mis à disposition par l'établissement tout en en étant pleinement administrateurs, que cet état de fait soit motivé par la nécessité professionnelle ou tout autre facteur.

Article 4 - Communications électroniques

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.

4.1 Messagerie électronique

L'utilisation de la messagerie constitue l'un des éléments essentiels d'optimisation du travail et de mutualisation de l'information au sein de CentraleSupélec.

La messagerie est un outil destiné à des usages professionnels :

- elle peut constituer le support d'une communication privée dans les limites définies à la section 2.1 ;
- elle est soumise aux recommandations de la charte numérique, au même titre que les autres outils de travail.

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 s'ils ne sont pas marqués comme « privée ». Ce contrôle est limité uniquement aux boîtes aux lettres professionnelles.

De plus des applications anti-spam et antivirus peuvent mettre en quarantaine certains messages quand ceux-ci sont analysés à risque.

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 personnel conformément à l'article 2.1, ou s'ils ne sont pas identifiés comme échangés dans le cadre d'une fonction de représentant du personnel, syndicale ou associative de l'école.

(a) Adresses électroniques

CentraleSupélec s'engage à mettre à la disposition de l'utilisateur une boîte à lettres professionnelle nominative lui permettant d'émettre et de recevoir des messages électroniques.

Dans la mesure du possible, l'adresse électronique attribuée par l'administration à chaque personnel de CentraleSupélec prend la forme prenom.nom@centralesupelec.fr, sauf cas particuliers ou situations d'homonymie.

De la même manière, l'adresse électronique attribuée par l'administration aux étudiants de CentraleSupélec prend, si possible, la forme prenom.nom@student-cs.fr, sauf cas particuliers ou situations d'homonymie.

L'aspect nominatif de l'adresse électronique constitue le simple prolongement de l'adresse administrative : il ne retire en rien le caractère professionnel de la messagerie.

L'adresse électronique nominative est attribuée à un utilisateur qui peut autoriser, à son initiative et sous sa responsabilité, l'accès de tiers à sa boîte à lettres via des moyens techniques permettant d'éviter de devoir partager son mot de passe (le support informatique de la DISI peut aider à mettre cela en place). Dans ce cas, le tiers est un personnel ou étudiant de CentraleSupélec.

Une adresse électronique, fonctionnelle ou organisationnelle, peut être mise en place si elle est exploitée par un service ou un groupe d'utilisateurs.

La gestion d'adresses électroniques correspondant à des listes de diffusion institutionnelles, désignant une catégorie ou un groupe d'« utilisateurs », relève de la responsabilité exclusive de CentraleSupélec : ces adresses ne peuvent pas être utilisées sans autorisation explicite.

(b) Contenu des messages électroniques

Les messages électroniques permettent d'échanger des informations à vocation professionnelle liées à l'activité de CentraleSupélec ou au sein de CentraleSupélec. En toutes circonstances, l'utilisateur doit adopter un comportement responsable et respectueux des dispositions contenues dans la présente charte.

Il convient de rappeler que la messagerie ne saurait être utilisée afin de commettre une quelconque infraction à la législation, que ce soit par les contenus véhiculés ou les propos qui y seraient échangés (tels que la diffamation, la discrimination, les propos racistes…). Elle ne saurait en outre comporter des contenus susceptibles de mettre en péril la sécurité du système d'information (ex : pièces jointes trop lourdes ou à risques).

Les auteurs de messages contenant de telles mentions sont susceptibles de faire l'objet de poursuites pénales ainsi que de poursuites disciplinaires par l'établissement.

Par référence à l'article 2.1, tout message est réputé professionnel sauf s'il comporte en objet la mention « privé », « personnel », « private », « personal » ou s'il est stocké dans un espace spécifique de données identifié comme tel.

Pour garantir la confidentialité des données échangées, l'utilisateur doit s'assurer de l'identité et de l'exactitude des adresses des destinataires des messages.

Pour la même raison, il doit veiller à ce que la diffusion des messages soit limitée aux seuls destinataires concernés.

Il convient également de préciser que comme toutes les informations traitées sur le système d'information de CentraleSupélec, la messagerie de chacun est présumée professionnelle. Cela n'empêche pas qu'elle soit personnelle et confidentielle, mais pour des raisons de sécurité et de protection de notre patrimoine immatériel, elle doit rester maitrisée par CentraleSupélec à qui elle appartient.
Il est donc formellement interdit de mettre en œuvre une redirection automatique des messages reçus dans votre boîte aux lettre de CentraleSupélec vers une messagerie personnelle externe (exemple : @gmail.com ; @free.fr, etc.) ou vers une messagerie professionnelle externe à CentraleSupélec. Une seule exception à cette règle peut s'appliquer si vous êtes vous-même dans une équipe commune avec un de nos partenaires institutionnels (exemple : CNRS, INRIA, Université Paris Saclay, ENS, etc.) en tant que chercheur, enseignant ou élève. Dans ce dernier cas, il sera possible de demander l'accord de la DISI pour la mise en place de cette redirection.

(c) Statut et valeur juridique des messages

L'ordonnance n° 2005-674 du 16 juin 2005 permet désormais l'accomplissement par voie électronique de certaines formalités exigées par le droit commun des contrats, et complète par ailleurs le dispositif visant à reconnaître les contrats sous forme électronique.

(d) Stockage et archivage des messages

Chaque utilisateur doit organiser et assurer la conservation des messages pouvant être indispensables à l'exercice de ses activités ou simplement utiles en tant qu'éléments de preuve.

4.2 Internet

Il est rappelé que le réseau Internet est soumis à l'ensemble des règles de droit en vigueur.

CentraleSupélec met à la disposition de l'utilisateur un accès Internet chaque fois que cela est possible.

Internet est un outil de travail destiné à des usages professionnels : il peut constituer le support d'une communication privée telle que définie en 2.1, dans le respect de la réglementation en vigueur.

Les utilisateurs sont informés qu'en considération de la mission éducative de l'établissement, la consultation volontaire de contenus illicites depuis les locaux ou via les moyens numériques de CentraleSupélec est proscrite.

CentraleSupélec se réserve le droit de filtrer ou d'interdire l'accès à certains sites, de procéder au contrôle a priori ou a posteriori des sites visités et des durées d'accès correspondantes. L'utilisateur en est dans ce cas informé.

L’accès à Internet n'est autorisé qu'au travers des dispositifs de sécurité mis en place par CentraleSupélec.

L'utilisateur est informé des risques et limites inhérents à l'utilisation d'Internet, par le biais d'actions de formation ou de campagnes de sensibilisation, relayées notamment via l’environnement numérique et social de travail.

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 à nos obligations réglementaires pour répondre aux éventuelles injonctions de la justice.

4.3 Téléchargements

Tout téléchargement de fichiers, notamment de sons ou d’images, doit s'effectuer dans le respect des droits de propriété intellectuelle tels que définis à l'Article 6 -

CentraleSupélec se réserve le droit de limiter le téléchargement de certains fichiers pouvant se révéler volumineux ou présenter un risque pour la sécurité des systèmes d'information, tels les virus, les codes et scripts malveillants ou les programmes espions.

4.4 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 ainsi que les numéros surtaxés et les appels à l’étranger en cas d’usage abusif.

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.

Article 5 - Traçabilité

CentraleSupélec est dans l'obligation légale de mettre en place un système de journalisation des accès Internet, de la messagerie et des données échangées.

CentraleSupélec se réserve le droit de mettre en place des dispositifs de traçabilité sur tous les outils et services numériques qu’elle met à la disposition des utilisateurs.

Conformément au Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 (RGPD)

et à la loi n° 78-17 du 6 janvier 1978 dite « Informatique et Libertés » modifiée, ce traitement de données est inscrit au registre des traitements de l'établissement.

Les utilisateurs sont informés que la durée légale de conservation des fichiers de journalisation est d'une année à partir de la date d'enregistrement.

Article 6 - Respect de la propriété intellectuelle

Général :

CentraleSupélec rappelle que l'utilisation des moyens numériques implique le respect de ses droits de propriété intellectuelle ainsi que ceux de ses partenaires et, plus généralement, de tous tiers titulaires de tels droits.

En conséquence, chaque utilisateur doit :

- utiliser les logiciels, bases de données, pages web, textes, images, photographies ou autres créations protégées par le droit d'auteur dans le strict respect des licences qui leur sont attachées ;
- s'abstenir de reproduire, copier, diffuser, modifier, sans avoir obtenu préalablement et personnellement le cas échéant, si requis, l'autorisation du ou des titulaires des droits de propriété intellectuelle.

Dispositif anti-plagiat :

Dans le cadre de sa démarche de mise en place d'outils de prévention et de détection du plagiat, CentraleSupélec met à disposition de ses enseignants-chercheurs et enseignants un logiciel de détection de similitudes.

Ce service permet d'analyser des travaux rendus par les étudiants sous forme numérique, pour repérer et identifier des paragraphes similaires à des textes disponibles en ligne ou dans les bibliothèques de référence et dont les sources ne seraient pas citées.

CentraleSupélec informe ses étudiants que leurs productions (rapport de stage, mémoire, thèse, etc.) sont susceptibles d'être analysées par la solution de détection de similitudes.

Un acte de plagiat peut constituer le délit de contrefaçon engageant la responsabilité civile, voire pénale, du plagiaire par infraction à la réglementation en matière de propriété intellectuelle. Cette pratique constitue également une infraction au règlement des examens de CentraleSupélec, passible de sanctions disciplinaires pour fraude aux examens, décidées par la section disciplinaire compétente conformément aux dispositions du code de l'éducation (articles R811-11 et suivants).

Le signataire de la présente charte s'engage sur l'honneur au respect de la réglementation en matière de propriété intellectuelle, ainsi qu'au respect des règlements intérieurs de CentraleSupélec.

Article 7 - Protection des données à caractère personnel

L'utilisateur est informé de la nécessité de respecter la réglementation en matière de traitements (automatisés

ou non) de données à caractère personnel, conformément au Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 (RGPD) et à la loi n° 78-17 du 6 janvier 1978 dite « Informatique et Libertés » modifiée.

Une donnée à caractère personnel est toute information relative à une personne physique susceptible d'être identifiée directement ou indirectement.

Tout traitement impliquant des données à caractère personnel doit être conforme aux dispositions du RGPD et de la loi n°78-17 du 6 janvier 1978 dite « informatique et libertés » modifiée. Sont notamment considérés comme des traitements les opérations suivantes : l'enregistrement, la conservation, la diffusion de données à caractère personnel sur support numérique ou papier. Sont également soumis à la réglementation les systèmes de vidéosurveillance.

En conséquence, tout utilisateur souhaitant procéder à un tel traitement devra en informer préalablement le délégué à la protection des données (DPO) qui prendra les mesures nécessaires au respect des dispositions légales.

Par ailleurs, conformément aux dispositions de cette loi, chaque utilisateur dispose d'un droit d'accès, de rectification et d'opposition relatif à l'ensemble des données le concernant, y compris les données portant sur l'utilisation des systèmes d'information. Selon les cas l'utilisateur dispose également d'un droit à la limitation du traitement et à la portabilité de ses données.

Ces droits s'exercent auprès du délégué à la protection des données (DPO) de l'établissement : dpo@centralesupelec.fr

Il est à noter que la création d'un compte informatique CentraleSupélec peut entrainer un partage de données personnelles avec :

- le personnel de CentraleSupélec habilité et ayant en charge le traitement de vos données dans le cadre de leur fonction (SGAE, direction des études, service d'accompagnement des élèves, DRH, Service financier, etc.)
- l'Université Paris-Saclay (dont CentraleSupélec est membre) pour des raisons de mutualisation des services comme la bibliothèque ou de mise en place de parcours pédagogiques à travers différents établissement de l'Université Paris-Saclay comme par exemple les masters et les études doctorales ;
- des établissements partenaires autres que ceux de l'Université Paris-Saclay dans des parcours pédagogiques spécifiques ;
- les associations des élèves de CentraleSupélec pour communiquer avec l'ensemble des élèves et aider les nouveaux entrants ;
- des partenaires ou des sous-traitants pour des activités spécifiques et limitées (ex. l'association Césal pour la résidence des élèves)

S'il y a partage de données personnelles, CentraleSupélec s'engage à s'assurer que l'autre partie se conformera aux exigences du RGPD et que ces données ne seront pas utilisées à des fins commerciales ou autres que ceux définis par des exigences pédagogiques, organisationnelles ou réglementaires.

Article 8 – Droits et obligations des Administrateurs

8.1 Définition : Administrateur :

Le terme « administrateur » désigne tout agent ayant pour mission d'assurer le bon fonctionnement ou la

sécurité des ressources des systèmes d'information placées sous sa responsabilité dont, notamment, les serveurs, les équipements réseaux, la téléphonie, les équipements de sécurité, les applications, les bases de données ou les postes de travail.

La présente charte s'adresse à tout administrateur, quel que soit son statut : titulaire ou contractuel, ainsi que tout consultant ou prestataire.

Pour l'exécution de sa mission, l'administrateur dispose de droits d'accès privilégiés susceptibles de lui permettre l'accès à des informations, tels que des courriels, des fichiers, des données de connexion confidentielles ou non, à caractère privé ou professionnel, dont il n'est ni le destinataire, ni l'auteur, ni le propriétaire.

Ces droits d'accès privilégiés lui permettent aussi d'entreprendre des actions potentiellement dangereuses pour les systèmes d'information telles que, par exemple, la modification ou le contournement de mécanismes de protection, la création ou la modification de comptes utilisateurs, la destruction ou la modification de fichiers.

L'administrateur est tenu au secret professionnel et soumis à l'obligation de discrétion professionnelle, il exerce ses missions dans le respect des prescriptions règlementaires régissant son statut, excluant de fait toute utilisation de ses droits d'accès privilégiés à des fins personnelles.

8.2 : Droits de l'administrateur

Dans le cadre de ses missions, un administrateur a le droit :

- d'interrompre le fonctionnement de tout équipement, logiciel ou matériel, qui compromettrait la sécurité ou le bon fonctionnement d'un - ou d'un ensemble de – système(s) d'information ;
- d'utiliser des données et d'accéder à des informations privées à des fins de traitement lié à sa mission, de diagnostic, de vérification, de statistiques ou en cas d'anomalie ou d'incident ;
- de prendre les mesures adéquates afin de prévenir tout risque de sécurité tel que virus, intrusion ou vol de données, destruction de données ou contournement de la politique de sécurité.

8.3 : Devoirs de l'administrateur

Dans le cadre de ses missions, un administrateur :

- ne prend pas connaissance de données personnelles d'utilisateurs - sauf ponctuellement, sur demande formelle de l'utilisateur lui-même ou à travers sa mission (RH, Finance, SGAE, etc.)- et n'autorise quiconque à y accéder, sauf cas particuliers prévus par la loi ;
- respecte les dispositions mentionnées dans la charte numérique auxquelles sont soumis les administrateurs dans l'exercice de leurs missions, en particulier sur le traitement des informations privées, sur la messagerie, sur le réseau Internet, sur la traçabilité, sur les mesures de contrôle et l'obligation d'information des utilisateurs ;
- respecte scrupuleusement la confidentialité des informations auxquelles il a accès et met en œuvre des mesures visant à assurer leur non divulgation ;
- s'assure, avec le délégué à la protection des données (DPO@centralesupelec.fr) désigné, que la mise en œuvre du traitement respecte la règlementation sur la protection des données à caractère personnel ;
- informe le Responsable de la Sécurité des Systèmes d'Information (RSSI@centralesupelec.fr) de tout incident de sécurité dont il pourrait avoir connaissance ;
- n'utilise ses droits d'accès privilégiés qu'exclusivement pour les activités et les besoins directement liés à ses missions, et en aucun cas à des fins personnelles ;
- agit dans le sens d'une meilleure sécurité, dans l'intérêt de l'établissement et des utilisateurs.
- s'engage à respecter en toutes circonstances la législation en vigueur et le règlement intérieur de

CentraleSupélec incluant les dispositions de la présente charte

Article 9 - Limitations des usages

En cas de non-respect par un utilisateur ou un administrateur des règles définies dans la présente charte et des modalités présentées dans le guide pratique annexé, le Directeur Général des Services pourra, après en avoir averti l'intéressé et sans préjuger des poursuites ou procédures de sanction pouvant être engagées à son encontre, limiter les usages suivants par mesure conservatoire :

- limiter les accès de l'utilisateur ;
- déconnecter l'utilisateur, avec ou sans préavis selon la gravité de la situation ;
- retirer les codes d'accès ou autres dispositifs de contrôle d'accès et fermer les comptes ;
- effacer, compresser ou isoler toute donnée ou fichier trop lourd, ou manifestement en contradiction avec la charte, ou qui mettrait en péril la sécurité des ressources ;
- interdire à l'utilisateur tout accès aux ressources dont il est responsable.

Tout abus dans l'utilisation à des fins extraprofessionnelles des ressources mises à la disposition de l'utilisateur est passible des sanctions définies dans l'article 10.

Article 10 - Manquements

Les non-respects de la charte numérique 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).

Les principales sanctions disciplinaires applicables aux utilisateurs du réseau informatique sont :

- Loi n°84-16 du 11 janvier 1984 Article 66 portant dispositions statutaires relatives à la fonction publique de l'Etat ;
- Code de l'éducation Articles R811-11 et suivants ainsi que les Articles 952-8 et suivants ;
- Décret n° 86-83 du 17 janvier 1986 Article 43-2 relatif aux dispositions générales applicables aux agents contractuels de l'Etat

L'établissement peut engager une procédure disciplinaire à l'encontre d'un utilisateur en infraction avec la charte numérique, cela quel que soit le statut de ce dernier, usager ou personnel (administratif titulaire ou contractuel, enseignant-chercheur, membres des corps des personnels enseignants de l'enseignement supérieur et autres enseignants), et indépendamment des poursuites pénales qui pourraient être engagées à son encontre.

La procédure disciplinaire à l'encontre des usagers peut déboucher sur des sanctions allant de l'avertissement à l'exclusion de l'établissement, avec sursis ou non, ou l'exclusion de tout établissement d'enseignement supérieur public (article R811-36 du code de l'éducation).

Les sanctions applicables aux enseignants-chercheurs et aux membres des corps des personnels enseignants de l'enseignement supérieur sont édictées par l'article L952-8 du code de l'éducation qui prévoit 7 niveaux de sanctions, du blâme (1er niveau) à la révocation (7ème niveau). Deux sanctions intermédiaires étant l'abaissement d'échelon (3ème niveau) et l'interdiction d'exercer toutes fonctions d'enseignement ou de recherche ou certaines d'entre elles dans l'établissement ou dans tout établissement public d'enseignement

supérieur pendant cinq ans au maximum, avec privation de la moitié ou de la totalité du traitement (5ème niveau).

Les sanctions applicables aux autres enseignants (article L952-9 du code de l'éducation) sont classées en 4 niveaux: la sanction la moins élevée est le rappel à l'ordre, la plus élevée est l'interdiction d'exercer des fonctions d'enseignement ou de recherche dans tout établissement public d'enseignement supérieur soit pour une durée déterminée, soit définitivement. Les sanctions intermédiaires étant l'interruption de fonctions dans l'établissement pour une durée maximum de deux ans (2ème niveau) et l'exclusion de l'établissement (3ème niveau).

Les personnels ingénieurs, administratifs, techniques, ouvriers et de service titulaires peuvent se voir infliger les sanctions prévues par la loi n° 84-16 du 11 janvier 1984 (article 66), celles-ci sont classées par groupes : l'exclusion temporaire de fonctions pour une durée maximale de trois jours (dernière sanction du 1er groupe) ; le déplacement d'office (dernière sanction du 2ème groupe) ; l'exclusion temporaire de fonctions pour une durée de seize jours à deux ans (dernière sanction du 3ème groupe) ; la révocation (dernière sanction du 4ème groupe).

Les sanctions applicables aux agents administratifs contractuels sont les suivantes (article 43-2 Décret n° 86-83 du 17 janvier 1986 relatif aux dispositions générales applicables aux agents contractuels de l'État)

1. L'avertissement ;
2. Le blâme ;
3. L'exclusion temporaire des fonctions avec retenue de traitement pour une durée maximale de six mois pour les agents recrutés pour une durée déterminée et d'un an pour les agents sous contrat à durée indéterminée ;
4. Le licenciement, sans préavis ni indemnité de licenciement.

Article 11 - Entrée en vigueur de la charte

11.1) Compte tenu de la consultation préalable des représentants du personnel ainsi que de l'approbation de cet Charte en, annexe du règlement intérieur par le CA, la présente charte entrera en vigueur à compter du 17/06/2022.

11.2) 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 CentraleSupélec.

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