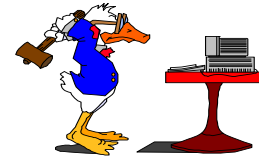




Nom :

Prénom :



CHARTRE DE BON USAGE DES RESSOURCES INFORMATIQUES

Préambule

Les outils informatiques mis par SUPÉLEC à la disposition de ses étudiants n'échappent pas aux règles normales de bon usage telles que précautions d'emploi, utilisation exclusive dans le cadre défini par SUPÉLEC, respect des droits de l'Ecole, des tiers et de l'ordre public.

Plus largement, la généralisation de l'outil informatique dans le quotidien des étudiants, nécessite de rappeler quelques règles, aussi bien pour éviter de se mettre en infraction, que pour se protéger et protéger les tiers.

Ce texte, qui constitue un pan du Règlement intérieur de l'Etablissement, est destiné à informer, sensibiliser et responsabiliser les utilisateurs quant à leurs droits et obligations.

Précautions et bonne conduite

Des négligences personnelles peuvent mettre en péril tout le travail d'une collectivité : la responsabilité de chacun est seule garante de la tranquillité de tous. Il est nécessaire à la fois de se protéger des agressions potentielles, de protéger les ressources communes et aussi de se conformer à une attitude de solidarité envers les autres utilisateurs. Par exemple, on devra obligatoirement :

- **utiliser des mots de passe efficaces** (*mélange sans signification de lettres minuscules et majuscules et de chiffres*), tenus rigoureusement confidentiels et personnels, changés régulièrement,
- **toujours se déconnecter en fin d'utilisation,**
- **s'interdire d'introduire sur les ressources informatiques communes des éléments** (*disquettes, fichiers binaires, ...*) **que l'on peut suspecter d'être porteurs de virus ou d'autres sources d'agressions.**
- **respecter scrupuleusement les consignes données dans un document joint sur la non réponse à l'hameçonnage (*phishing*).**

Utilisation responsable des ressources

Les ordinateurs, le réseau, les imprimantes, les disques où sont stockées les boîtes à lettres électroniques sont des dispositifs partagés par l'ensemble de la communauté SUPÉLEC dans le cadre des activités quotidiennes. En aucun cas, ils ne peuvent être considérés comme un terrain d'expériences ou de jeux. Bien que les logiciels utilisés aient été conçus pour faire fonctionner l'ensemble avec une fiabilité maximum dans des conditions de charge très importante, une utilisation abusive peut entraîner des dysfonctionnements nuisibles à tous en provoquant des interruptions du service.

Il est donc rappelé que **les ordinateurs, les logiciels, le réseau Internet et ses différentes fonctionnalités** (email, web, transfert de fichiers) **ne peuvent être utilisés que pour les besoins professionnels**, tel que l'enseignement et la recherche, voire personnels pour la communication. Il est

formellement interdit de les utiliser pour des besoins commerciaux ou promotionnels pour des entreprises externes.

Il est formellement interdit d'installer sur son ordinateur un logiciel de type « serveur » (comme le peer-to-peer ou toute autre activité prohibée par la loi), offrant donc certaines fonctionnalités à d'autres utilisateurs en local ou sur Internet.

Il est formellement interdit d'utiliser les listes de distributions électroniques pour faire du prosélytisme politique, syndical ou religieux.

Le réseau informatique ne doit pas être utilisé pour effectuer et/ou promouvoir des actions de vente ou de revente de bien et/ou services, notamment lorsqu'ils sont soumis à des législations spécifiques (ex: vente de tabac ou de boissons, liste non exhaustive).

Il est formellement interdit de brancher son ordinateur personnel sur une prise réseau de l'Ecole.

Les étudiants sont informés que le responsable du site est inscrit sur les listes de distribution des élèves et peut participer à toute discussion ou faire état des emails transmis, pouvant ainsi agir comme modérateur du site.

Aussi, les ressources mises à la disposition des étudiants ne le sont que pendant leur scolarité à SUPELEC. Les comptes seront donc fermés à la fin de cette scolarité et les fichiers divers et variés, ainsi que les boîtes à lettres seront détruites à ce moment-là.

En cas de non utilisation prolongée du courrier électronique, le responsable du site se réserve le droit d'effacer les messages non lus, reçus depuis plus d'un mois.

Une liste de recommandations est jointe à ce document.

Pratiques prohibées

Infractions en matières informatiques

Article 323-1 du Code pénal : *Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 30 000 euros d'amende. Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de 45 000 euros d'amende.*

Article 323-2 du Code pénal : *Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de cinq ans d'emprisonnement et de 75 000 euros d'amende.*

Article 323-3 du Code pénal : *Le fait d'introduire frauduleusement des données dans un système de traitement automatisé ou de supprimer ou de modifier frauduleusement les données qu'il contient est puni de cinq ans d'emprisonnement et de 75 000 euros d'amende.*

Article 323-3-1 du Code pénal : *Le fait, sans motif légitime, d'importer, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre une ou plusieurs des infractions prévues par les articles 323-1 à 323-3 est puni des peines prévues respectivement pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée.*

Article 323-4 du Code pénal : *La participation à un groupement formé ou à une entente établie en vue de la préparation, caractérisée par un ou plusieurs faits matériels, d'une ou de plusieurs des infractions prévues par les articles 323-1 à 323-3-1 est punie des peines prévues pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée.*

Article 226-15 du Code pénal : *Le fait, commis de mauvaise foi, d'ouvrir, de supprimer, de retarder ou de détourner des correspondances arrivées ou non à destination et adressées à des tiers, ou d'en prendre frauduleusement connaissance, est puni d'un an d'emprisonnement et de 45 000 euros d'amende.*

Est puni des mêmes peines le fait, commis de mauvaise foi, d'intercepter, de détourner, d'utiliser ou de divulguer des correspondances émises, transmises ou reçues par la voie des télécommunications ou de procéder à l'installation d'appareils conçus pour réaliser de telles interceptions.

Données personnelles

Article 226-21 du Code pénal : *Le fait, par toute personne détentrice de données à caractère personnel à l'occasion de leur enregistrement, de leur classement, de leur transmission ou de toute autre forme de traitement, de détourner ces informations de leur finalité telle que définie par la disposition législative, l'acte réglementaire ou la décision de la Commission nationale de l'informatique et des libertés autorisant le traitement automatisé, ou par les déclarations préalables à la mise en œuvre de ce traitement, est puni de cinq ans d'emprisonnement et de 300 000 Euros d'amende.*

Propriété intellectuelle

Article L. 335-2 du Code de la propriété intellectuelle : *Toute édition d'écrits, de composition musicale, de dessin, de peinture ou de toute autre production, imprimée ou gravée en entier ou en partie, au mépris des lois et règlements relatifs à la propriété des auteurs, est une contrefaçon et toute contrefaçon est un délit.*

La contrefaçon en France d'ouvrages publiés en France ou à l'étranger est punie de trois ans d'emprisonnement et de 300 000 euros d'amende.

Article L. 335-2-1 du Code de la propriété intellectuelle : *Est puni de trois ans d'emprisonnement et de 300 000 euros d'amende le fait :*

1° d'éditer, de mettre à la disposition du public ou de communiquer au public, sciemment et sous quelque forme que ce soit, un logiciel manifestement destiné à la mise à disposition du public non autorisée d'œuvres ou d'objets protégés ;

2° d'inciter sciemment, y compris à travers une annonce publicitaire, à l'usage d'un logiciel mentionné au 1°.

Article L. 335-3 du Code de la propriété intellectuelle : *Est également un délit de contrefaçon toute reproduction, représentation ou diffusion, par quelque moyen que ce soit, d'une œuvre de l'esprit en violation des droits de l'auteur, tels qu'ils sont définis et réglementés par la loi.*

Est également un délit de contrefaçon la violation de l'un des droits de l'auteur d'un logiciel définis à l'article L. 122-6.

Est également un délit de contrefaçon toute captation totale ou partielle d'une œuvre cinématographique ou audiovisuelle en salle de spectacle cinématographique.

Article L. 335-3-1 du Code de la propriété intellectuelle : *I. - Est puni de 3 750 euros d'amende, le fait de porter atteinte sciemment, à des fins autres que la recherche, à une mesure technique efficace telle que définie à l'article L. 331-5, afin d'altérer la protection d'une œuvre par un décodage, un décryptage ou toute autre intervention personnelle destinée à contourner, neutraliser ou supprimer un mécanisme de protection ou de contrôle, lorsque cette atteinte est réalisée par d'autres moyens que l'utilisation d'une application technologique, d'un dispositif ou d'un composant existant mentionné au II.*

II. - Est puni de six mois d'emprisonnement et de 30 000 euros d'amende, le fait de procurer ou proposer sciemment à autrui, directement ou indirectement, des moyens conçus ou spécialement adaptés pour porter atteinte à une mesure technique efficace telle que définie à l'article L. 331-5, par l'un des procédés suivants :

1° En fabriquant ou en important une application technologique, un dispositif ou un composant, à des fins autres que la recherche ;

2° En détenant en vue de la vente, du prêt ou de la location, en offrant à ces mêmes fins ou en mettant à disposition du public sous quelque forme que ce soit une application technologique, un dispositif ou un composant ;

3° En fournissant un service à cette fin ;

4° En incitant à l'usage ou en commandant, concevant, organisant, reproduisant, distribuant ou diffusant une publicité en faveur de l'un des procédés visés aux trois alinéas précédents.

III. - Ces dispositions ne sont pas applicables aux actes réalisés à des fins de sécurité informatique, dans les limites des droits prévus par le présent code.

Il est par ailleurs rappelé que le nom SUPÉLEC, ainsi que son logo sont la propriété exclusive de l'Ecole. Il est donc strictement défendu sans l'autorisation écrite de l'Ecole:

- d'utiliser le nom ou le logo de SUPÉLEC à quelque fin que ce soit et sur quelque support que ce soit par exemple, sans que cette liste soit exhaustive, sur les forums internet externes à SUPÉLEC et sur les sites communautaires.
- de réserver un nom de domaine comprenant le nom SUPÉLEC.

Par ailleurs, tout logiciel développé dans un cadre scolaire, et non soumis à une convention spécifique, reste la propriété entière et totale de l'Ecole.

Respect d'autrui, Image de l'Ecole, de ses émanations et de ses intervenants

Le respect d'autrui est la règle de base d'utilisation de ressources communes. Aussi, rappelons que **la réputation de la formation dispensée et sanctionnée par SUPÉLEC procède notamment de son image auprès des tiers.**

L'attention est donc attirée sur le fait que dans ses échanges (courriels ou forums notamment), nul ne peut s'exprimer au nom de l'École ou engager l'École sans y avoir été dûment autorisé. Par ailleurs, **les utilisateurs doivent être particulièrement vigilants quant aux propos tenus, notamment sur internet, qui impliqueraient l'École, ses émanations, ses étudiants ou son personnel** (prohibition de la diffamation, des injures...). Les utilisateurs doivent également veiller à ne pas publier de photographies de personnes sans qu'elles l'aient expressément autorisé.

Par ailleurs, sont strictement prohibées les utilisations contraires aux lois et règlements en vigueur et notamment celles qui ont pour objet ou pour effet la diffusion d'idéologies politiques, raciales ou religieuses, ou qui sont de nature à porter atteinte à l'ordre public, aux bonnes mœurs, à la dignité ou à la vie privée des personnes.

Informatique et Libertés

La fonction du Centre de Ressources Informatiques consiste, notamment, à veiller à la bonne marche des sites internet et intranet de SUPÉLEC dans tous leurs aspects et en particulier à empêcher ou détecter toute forme de piratage ou d'utilisation irrégulière des ressources.

Pour cela, les utilisateurs sont informés, que le personnel de l'Ecole a la possibilité, si nécessaire, d'aller consulter des fichiers journaux qui contiennent la liste (pas le contenu) de tous les échanges d'information effectués sur le réseau. Par exemple, qui a envoyé un email à qui à quelle heure, qui a reçu un email de qui à quelle heure.

Plus largement, les utilisateurs sont informés que des fichiers contenant des informations personnelles les concernant sont régulièrement créés par l'Ecole. SUPÉLEC a effectué les déclarations et obtenu les autorisations requises auprès de la Commission Nationale de l'Informatique et des Libertés (CNIL) pour créer ces fichiers et traiter les données personnelles qu'ils contiennent.

En application des articles 38 à 40 de la Loi Informatique et Libertés du 6 janvier 1978 modifiée, les utilisateurs bénéficient d'un droit d'accès, de rectification et de suppression des informations qui les concernent. Ce droit peut être exercé en en faisant la demande par courrier électronique à l'adresse suivante :

cil-supelec@supelec.fr

Responsabilité des utilisateurs

Les étudiants sont responsables de l'utilisation qu'ils font des ressources informatiques. Ils sont informés qu'en cas de non-respect de l'interdiction du téléchargement illicite d'œuvres de l'esprit
Document juin 2011

protégées, d'atteinte à un autre droit de propriété intellectuelle, d'atteinte à la vie privée ou en cas d'infraction de presse, seule leur responsabilité civile et/ou pénale pourra être engagée, sans que celle de SUPÉLEC puisse être recherchée.

Sanction des manquements à la présente Charte

Les étudiants sont informés qu'en cas de manquement à la présente Charte, outre les sanctions civiles et/ou pénales pouvant en découler, l'Ecole se réserve le droit :

- **d'interdire l'accès aux ressources informatiques, y compris au réseau de la Résidence, pendant une période allant de plusieurs jours à une interdiction définitive ;**
- **de sanctionner disciplinairement l'étudiant fautif, sanction pouvant aller jusqu'à l'exclusion définitive de l'étudiant.**

Engagement

Je soussigné(e), _____, déclare avoir pris connaissance de la Charte de bon usage des ressources informatiques de SUPÉLEC et en accepter les termes.

Campus : Gif Rennes Metz

1ère année 2ème année 3ème année

Si 3ème A, Option :
Stagiaire Entité :

Mastère Spécialisé ou Master Recherche

Si Mastère ou Master, Sigle :

Autre (préciser qualité et entité) :

Je reconnais également avoir reçu le document sur les consignes pour ne pas répondre au *phishing*.

Fait à _____, le _____
Signature

RECOMMANDATIONS ANNEXEES A LA CHARTE DE BON USAGE DES RESSOURCES INFORMATIQUE

Il s'agit d'énoncer ici quelques recommandations élémentaires.

Il ne faut pas enregistrer son mot de passe (en particulier dans le programme servant à lire son courrier électronique) car il y a un risque non négligeable de l'oublier et c'est contraire aux principes de sécurité.

Le champ « Objet » d'un email doit toujours être rempli.

Le « pourrissage », c'est-à-dire l'envoi de courrier électronique sans véritable contenu à des listes est interdit, même s'il est signalé dans l'objet du message.

La « réponse à tous » au lieu d'une réponse à l'expéditeur peut être considérée comme le pourrissage. 99% des emails reçus par ces listes sont conservés sans être lus pour un éventuel usage ultérieur. Le 1% restant est lu car le sujet n'est pas sans rapport avec ce qui est décrit ci-dessus avec comme exemple classique : "Qui peut me fournir le CD du produit XXX?" sachant que XXX est un produit commercial pour lequel SUPÉLEC n'a pas acheté de licence spécifique.

Vous devez acquérir un logiciel anti-virus permettant ainsi d'assurer l'intégrité de votre poste de travail et la non contamination de la communauté.

Au cas où vous seriez victime d'un virus informatique ou d'un message vous demandant de transmettre impérativement une annonce de Virus, vous ne devez absolument pas envoyer cette information sur les listes de distribution mais prévenir le responsable informatique qui prendra les mesures nécessaires de prévention.

Il est également conseillé de consulter le site Web <http://www.symantec.com/avcenter/hoax.html> qui vous permettra d'obtenir toutes les informations que vous souhaitez et surtout de vous assurer que ce n'est pas une des nombreuses tentatives d'intoxication par courrier électronique interposé (hoax).

Pour éviter d'envoyer des courriers qui encombreront les boîtes à lettres, l'utilisation d'un Forum est fortement encouragée. Cela permet en outre de conserver l'historique des discussions.

Tout propos insultant vis-à-vis d'une personne, élève ou personnel, est évidemment proscrit. La promotion d'entreprises commerciales ou de sites Web cherchant à se constituer des fichiers d'étudiants par le biais de jeux plus ou bien dotés est interdite.

La transmission par email de fichiers volumineux ou la tentative d'en récupérer par Internet doit se faire avec certaines précautions en tenant compte des possibilités du site. Il est indispensable de commencer par regarder la taille du fichier que l'on souhaite envoyer. En cas de transmission de fichiers, précisez toujours le contenu du fichier à votre destinataire.

La diffusion sur les listes de distribution internes est contrôlée par l'adresse électronique de l'expéditeur. Toute usurpation d'identité pour atteindre ces listes ou envoyer un courrier électronique est contraire à la Charte.

L'inscription sur des listes de diffusion externes peut entraîner un afflux inattendu de messages. Il est donc fortement recommandé de se désabonner provisoirement de ces listes prolixes pendant les périodes de vacances.