

Accéder aux ressources numériques de L' ENSCM

Pour les personnels

Etre saisi dans le logiciel HARPEGE (attention le personnel doit être obligatoirement affecté à une structure)

Soit au service de relations Humaines

Soit auprès des gestionnaires de laboratoire

Avoir signé l'engagement de respect de la charte informatique.

Pour les Etudiants

Etre saisie dans le logiciel APOGEE

Avoir signé l'engagement de respect de la charte informatique.

Une fois la saisie effectuée, les identifiants sont créés et vérifiés par le logiciel développé autour de l'annuaire centralisé (LDAP). Une liste des comptes est créée et envoyée au service informatique à J+1.

Les informations de connexion seront transmises par la suite au responsable de service ou sur l'adresse mail personnelle des utilisateurs si celle ci nous est transmise.

Vous trouverez en dernière page une fiche d'engagement à compléter et signer.
Renvoyez là au service informatique. Par courrier ou par mail.

Service Informatique

ENSCM

8 Rue Ecole Normale

34296 Montpellier Cedex 5

svp@enscm.fr

Charte Informatique

La présente charte a pour objet de définir les règles d'utilisation des moyens informatiques au sein de l'établissement, de rappeler les responsabilités des utilisateurs et de leur faire prendre conscience que cette activité s'inscrit dans un cadre juridique précis assorti de sanctions pénales dont la gravité n'est pas la moindre des caractéristiques.

1.-Domaines d'application.

Les règles et obligations énoncées ci-dessous s'appliquent à tout utilisateur des ressources informatiques de l'Ecole : étudiant, stagiaires, enseignant, enseignant-chercheur, chercheur, personnel administratif ou technique.

Ces ressources comprennent les serveurs, les stations de travail et micro-ordinateurs et leurs périphériques, situés dans les locaux et les laboratoires de l'Ecole.

Les règles définies par la présente charte s'étendent également à l'utilisation des réseaux de l'établissement et des réseaux extérieurs accessibles par l'intermédiaire des réseaux de l'établissement.

L'utilisation du réseau RENATER est régie par une "Charte d'usage et de sécurité" que l'établissement s'est engagé à respecter.

Le non respect des règles engage la responsabilité personnelle de l'utilisateur.

L'établissement est lui-même soumis aux règles de bonne utilisation des moyens informatiques, et à ce titre il se doit de faire respecter les règles déontologiques et la loi.

Les diverses lois concernées par ce document sont présumées connues en particulier :

La loi Informatique et Libertés 92-684 du 22/7/1992 ;

La loi relative à la fraude informatique 92-685 du 22/7/1992 ;

Le code de la propriété intellectuelle 92-597 du 1/7/1992 ;

La loi relative aux infractions de presse du 29/7/1881, modifiée, sanctionnant notamment la diffamation, le négationnisme, le racisme et les injures ;

La loi relative aux infractions aux règles de cryptologie ; du 29/12/1990 modifiée le 26/7/1996.

2.-Autorisation d'accès aux serveurs et usage des ressources informatiques.

Le droit d'accès sur un serveur est temporaire. Il est retiré si la qualité de l'utilisateur ne le justifie plus.

Il peut également être retiré, par mesure conservatoire du Directeur de l'Ecole, si le comportement d'un utilisateur n'est plus compatible avec les règles énoncées dans la présente charte.

Le droit d'accès est limité à des activités conformes aux missions de l'établissement : la formation initiale et continue, la recherche scientifique et technologique ainsi que la valorisation de ses résultats, la diffusion de la culture et l'information scientifique et technique, la coopération internationale (article 4 de la loi numéro 84-52 du 26 janvier 1984).

Par ailleurs, l'étendue des ressources informatiques, auxquelles l'utilisateur a accès, peut être limitée en fonction des besoins réels et des contraintes imposées par le partage de ces ressources avec les autres utilisateurs.

Le droit d'accès est concrétisé par l'ouverture d'un compte personnel.

Obligations spécifiques aux titulaires de compte personnel : -

Un compte personnel est soumis à autorisation et inaccessibles.

A chaque compte personnel correspond un sigle d'identification unique auquel est associé un mot de passe.

Le titulaire d'un compte personnel est tenu de fournir des informations individuelles valides.

Il est également tenu de notifier aux gestionnaires de compte toute modification de ces informations,

la fourniture d'informations délibérément erronées est considérée comme une faute grave pouvant entraîner une interdiction d'accès aux ressources.

3.-Règles générales de sécurité.

Tout utilisateur est responsable de l'utilisation qu'il fait des ressources informatiques de l'Ecole. Il doit donc, à son niveau, contribuer à la sécurité. En particulier :

-Tout utilisateur doit choisir des mots de passe sûrs respectant les recommandations de l'administrateur système. Ces mots de passe doivent être gardés secrets, ne doivent pas être écrits et en aucun cas être communiqués à des tiers. A la demande des administrateurs système, ils doivent être changés.

-Tout utilisateur est responsable des possibilités d'accès à des informations situées sur des machines de l'ENSCM qu'il donne à un tiers, que ces accès puissent être établis en interne ou depuis l'extérieur. Cela concerne en premier lieu les propres fichiers de l'utilisateur mais cela concerne aussi, plus globalement, toute information à laquelle il a lui-même accès. En particulier, l'ouverture de service de type réseau (ftp, serveur Web) est subordonnée à l'accord d'un administrateur système et du responsable sécurité du site.

-Les utilisateurs ne doivent pas utiliser des comptes autres que ceux pour lesquels ils ont reçu une autorisation. Ils doivent s'abstenir de toute tentative de s'approprier ou de déchiffrer le mot de passe d'un autre utilisateur.

-L'utilisation, ou le développement de programmes, mettant sciemment en cause l'intégrité des systèmes informatiques de l'École ou des réseaux nationaux ou internationaux, est interdit.

-Tout constat de violation, tentative de violation ou soupçon de violation d'un système informatique doit être signalé à l'administrateur système de l'École.

-Les utilisateurs ne doivent pas abandonner de machine sans s'être préalablement déconnectés.

-Les utilisateurs doivent s'abstenir de toute tentative de falsification d'identité.

-Ils ne doivent pas ajouter de machines sur le réseau ailleurs que sur les prises autorisées par les administrateurs.

-En règle générale, un utilisateur doit être vigilant et signaler aux administrateurs système toute anomalie.

-Les utilisateurs sont tenus de respecter les consignes de l'administrateur système et des responsables informatiques.

-Les utilisateurs s'engagent à ne pas exploiter les éventuels vulnérabilités ou anomalies de fonctionnement. Ils doivent les signaler à l'administrateur système, et ne pas en faire la publicité. L'administrateur peut toutefois choisir de ne pas apporter de correction, si la correction n'est pas disponible ou est considérée comme induisant d'autres problèmes.

-Les utilisateurs évitent au mieux l'introduction et la propagation de virus sur les moyens informatiques.

-Tout utilisateur est responsable de la pérennité de ses fichiers et de l'intégrité de son espace de travail.

4.-Informatique et Libertés.

La loi 92-684 du 22 juillet 1992 protège tout individu contre tout usage abusif ou malveillant, d'informations le concernant et figurant dans un fichier informatique quelconque. Elle prévoit en particulier que :

- La création de tout fichier contenant des informations nominatives doit faire l'objet de formalités préalables à sa mise en oeuvre auprès de la Commission Nationale de l'Informatique et des Libertés (CNIL).
- Toute personne sur laquelle des informations figurent dans un tel fichier doit être informée de l'existence de ce fichier, de sa finalité, de l'existence d'un droit d'accès et des modalités de mise en oeuvre de celui-ci, dès la collecte des informations la concernant.

5.-Respect de la propriété intellectuelle.

L'utilisation des logiciels (source ou binaire) et plus généralement de tout document (fichier, image, son, etc.) doit se faire dans le respect de la propriété intellectuelle.

La copie d'un logiciel constitue le délit de contrefaçon sanctionné pénalement (loi 92-597 du 1er juillet 1992).

L'auteur d'une contrefaçon engage directement sa responsabilité :

- il peut être poursuivi devant les tribunaux répressifs et civils,
- la personne morale qui l'emploie, par exemple un établissement public, peut également être poursuivie.

-La reproduction de logiciel est, en général, interdite. Seul l'établissement d'une copie de sauvegarde pourra être autorisé si elle n'a pas déjà été assurée par les services compétents.

-Il est interdit d'installer sur un système de l'ENSCM un logiciel commercial quelconque, sans s'être assuré préalablement auprès du responsable des moyens informatiques du site que l'ENSCM y est autorisé.

L'utilisation des logiciels sur des réseaux ou sur des machines indépendantes se fera dans le respect des termes de la licence d'utilisation.

-L'utilisation permanente de logiciels à contribution volontaire (shareware) devra être signalée au responsable des moyens informatiques du site afin de régulariser rapidement cet usage. L'utilisateur s'engage à ne pas effectuer des opérations pouvant nuire au fonctionnement du réseau, à l'intégrité de l'outil informatique et aux relations internes et externes de l'établissement.

-La simple accession à un système sans autorisation constitue un délit, même s'il n'en est résulté aucune altération des données ou fonctionnement dudit système. Si de telles altérations sont constatées les sanctions prévues sont doublées (article 323-1 du nouveau code pénal).

-Les actes consistant à empêcher un système de fonctionner par exemple par l'introduction de "virus" sont visés par l'article 323-2 du nouveau code pénal.

-L'introduction ou la modification frauduleuse de données fait l'objet des articles 323-3 et 323-4 du nouveau code pénal.

-Il est à souligner que de tels actes (même de simples tentatives) sont susceptibles d'entraîner l'éviction de la fonction publique (article 323-5 du nouveau code pénal).

-Respect de la confidentialité des informations : La loi numéro 91-646 du 10 juillet 1991 stipule dans son article 2 : "Le secret des correspondances émises par la voie des télécommunications est garanti par la loi".

Ceci concerne le téléphone, le télécopieur, les liaisons informatiques et télématiques. De lourdes sanctions pénales frappent celui qui porte atteinte au secret de la correspondance (articles 226-15 et 432-9 du nouveau code pénal).

-Les utilisateurs ne doivent pas tenter de lire, de copier, de divulguer ou de modifier les fichiers d'un autre utilisateur sans y avoir été autorisés.

-Les utilisateurs doivent s'abstenir de toute tentative d'intercepter les communications privées, qu'il s'agisse de courrier électronique ou de dialogue direct.

-Les utilisateurs sont tenus à la réserve d'usage sur toute information relative au fonctionnement interne de l'ENSCM qu'ils auraient pu obtenir en utilisant ces ressources informatiques.

-Les utilisateurs sont tenus de prendre, avec l'aide éventuelle des responsables informatiques du site, les mesures de protection des données nécessaires au respect des engagements de confidentialité pris par l'ENSCM vis-à-vis de tiers.

6.-Autres obligations légales.

La loi prévoit que "les progiciels, les bases de données, les systèmes experts et les autres produits de l'intelligence artificielle sont soumis à l'obligation du dépôt légal dès lors qu'ils sont mis à la disposition du public".

Les produits réalisés au sein d'un service et mis à la disposition du public sont donc soumis à l'obligation du dépôt légal. Cette formalité doit être respectée sous peine de sanctions pénales (loi n 92-546 du 20 juin 1992).

La cryptologie est définie par l'article 28-1 de la loi numéro 90-1170 du 29 décembre 1990 : "On entend par prestation de cryptologie, toute prestation visant à transformer à l'aide de conventions secrètes des informations ou signaux clairs en informations ou signaux inintelligibles pour des tiers ou à réaliser l'opération inverse, grâce à des moyens matériels ou logiciels conçus à cet effet. On entend par moyen de cryptologie tout matériel ou logiciel conçu ou modifié dans le même objectif". Toute personne qui procède au codage d'un texte qu'elle entend transmettre par la voie de télécommunication doit respecter les procédures prévues par la loi, d'autorisation ou d'agrément préalable, sous peine de sanctions pénales. Le risque d'être en infraction n'est pas négligeable car la tentation est grande au sein d'un réseau de correspondants de convenir de coder les fichiers échangés.

Les informations diffusées par le biais des réseaux ne doivent pas :

-Porter atteinte à la vie privée ou à l'image d'autrui ;

-Contrevenir aux lois sur la propriété intellectuelle, littéraire et artistique ;

-Faire l'apologie du racisme, de l'antisémitisme et de la xénophobie, etc. (actes réprimés par les lois numéro 90-615 du 13 juillet 1990 et numéro 92-1336 du 16 décembre 1992).

7-Relations avec les autres sites informatiques et bon usage de la communication électronique.*

Dans ses échanges, nul ne peut s'exprimer au nom de l'École ou engager l'École sans y avoir été dûment autorisé.

Les installations de l'ENSCM permettant de se connecter ou de dialoguer avec des sites informatiques dans le monde entier, les accès aux autres sites doivent être faits dans le respect des règles d'usage propres aux divers sites et réseaux et dans le respect de la législation en vigueur comme la loi 92-685 du 22 juillet 1992 relative à la fraude informatique.

En particulier :

Il est interdit de se livrer depuis des systèmes appartenant à l'ENSCM ou connectés aux réseaux de l'ENSCM à des actions mettant sciemment en péril la sécurité ou le fonctionnement d'autres sites et des réseaux de télécommunications.

Il est interdit de se connecter ou d'essayer de se connecter sur un autre site sans y être dûment autorisé. On est autorisé à aller sur un site quand on dispose d'un compte sur ce site ou que l'on se limite aux services anonymes (ftp, WWW, etc.)

Les moyens informatiques de l'ENSCM permettent d'utiliser de nombreux supports de communication électronique (courrier, forums de discussion, documents accessibles par le WEB).

L'usage de ces supports de communication doit se faire dans le respect des règles suivantes :

-Chacun doit faire preuve de la plus grande correction dans ses communications quel que soit le service utilisé.

-Chacun doit veiller à ce que le contenu de ses communications soit conforme à la législation en vigueur.

-Chacun doit s'abstenir de porter atteinte par la nature de ses communications à l'image ou aux intérêts de l'ENSCM.

Droits et devoirs des administrateurs :

Les administrateurs désignés par le Directeur de ENSCM ont le devoir d'assurer un bon fonctionnement des réseaux et des moyens informatiques.

Ils ont le droit de prendre toutes dispositions nécessaires pour assumer cette responsabilité tout en respectant la déontologie professionnelle. En particulier, un administrateur peut prendre des mesures conservatoires (arrêt d'une exécution, suppression de droit d'accès,...) pour pallier un incident de fonctionnement ou de sécurité.

Dans ce cadre, il lui est licite de rechercher toute information utile, En particulier il peut explorer les fichiers des utilisateurs et en faire connaître des extraits à la Direction des départements et de l'École lorsqu'une telle recherche est rendue nécessaire par le constat d'actes de piratage. Il peut aussi générer et consulter tout journal d'événements, et enregistrer des traces, si besoin est.

Les administrateurs sont, au premier degré, les gestionnaires de comptes et de machines, et à un degré supérieur, le service qui gère l'accès aux réseaux et le Correspondant "sécurité informatique" du Ministère, désigné par le Directeur de l'École. Tout administrateur d'une ressource informatique, propre à un département, laboratoire ou service, doit déclarer au service Informatique la connexion de cette ressource au réseau.

Les utilisateurs peuvent demander l'aide des administrateurs pour faire respecter leurs droits. Sont « administrateurs-système » les personnes ayant les droits de « root » afin d'installer et de gérer les machines. Ils sont en charge d'assurer la meilleure marche possible du système pour tous.

Conclusion.

La sécurité est l'affaire de tous, c'est-à-dire chaque utilisateur de l'informatique et du réseau d'établissement. Les utilisateurs ne respectant pas les règles et obligations définies dans la présente charte et ceux qui ne signalent pas les tentatives de violation de leur compte sont passibles de sanctions :

Ils peuvent être sommairement déconnectés par les administrateurs qui peuvent surveiller en détail les sessions de travail d'un utilisateur s'il existe un soupçon de non respect de la charte.

Ils peuvent être traduits devant la Section disciplinaire du Conseil d'Administration de l'ENSCM en ce qui concerne les enseignants chercheurs, les chercheurs et les étudiants, et devant le Conseil de discipline de leur corps respectif en ce qui concerne les personnels administratifs et techniques.

Ils peuvent faire l'objet de poursuites pénales engagées à la demande de l'ENSCM.

Fait à Montpellier, Le 01 Mars 1998

Le Directeur



ENGAGEMENT

Je, soussigné(e),....., affecté(e)
à L'ENSCM, certifie avoir pris connaissance de la Charte Informatique de l'Ecole Nationale
Supérieure de Chimie de Montpellier et m'engage à m'y conformer strictement.

A Montpellier, le
Signature (Précédée de la mention manuscrite
«lu et approuvé».)

Laboratoire ou service :
Fonctions :
Tuteur ou Responsable :
Adresse mail personnel