École des Ponts
ParisTech

CHARTE D'UTILISATION DES MOYENS INFORMATIQUES

(Adoptée par le conseil d'administration du 15 décembre 1998)

1. DOMAINE D'APPLICATION DE LA CHARTE

1.1 MATERIELS, LOGICIELS ET SERVICES CONCERNES

La présente charte s'applique à tous les moyens informatiques locaux (serveurs, stations de travail, micro-ordinateurs), à tous les matériels de télécommunication (en particulier au téléphone et au Minitel), à tous les services accessibles à partir des machines locales directement ou en cascade (en particulier à tout l'Internet).

Dans ce qui suit, on désignera collectivement ces moyens sous le terme de système informatique.

1.2 LES UTILISATEURS

Un utilisateur est une personne habilitée à consommer des ressources informatiques ou téléphoniques de l'Ecole. Cette utilisation peut être liée aux activités d'enseignement, de recherche, d'expertise, de formation continue, d'administration, ou toute autre activité interne ou externe de l'Ecole. Les droits d'utilisation ne seront pas les mêmes selon les catégories de rattachement: ils seront précisés à chacun au moment de l'ouverture de leur compte de travail.

Cette charte s'applique également aux utilisateurs de matériels qui se connectent à partir de l'extérieur, notamment au moyen de modems.

1.3 LA DIRECTION DE L'INFORMATIQUE ET DES TELECOMMUNICATIONS (DIT)

Le schéma directeur de l'informatique et des télécommunications du 5 novembre 1991 définit les missions de la DIT, dont celles se rapportant à la coordination et à la mise en oeuvre des systèmes informatiques.

2. DROITS ET DEVOIRS DES UTILISATEURS

2.1 INFORMATIONS PERSONNELLES

Chaque utilisateur est tenu :

- de fournir des informations personnelles valides à l'administrateur compétent démontrant ses droits à utiliser les systèmes informatiques de l'Ecole et dans quel cadre,
- d'attester avoir pris connaissance de la charte.

Il recevra alors une identification unique ou multiple à laquelle sera associé un mot de passe (si possible) déterminant son droit d'accès à des ressources pour une durée déterminée.

Il est ensuite tenu de notifier à l'administrateur toute modification des informations personnelles fournies et en particulier toute circonstance entraînant la cessation de son droit d'usage.

2.2 CONDITIONS D'ACCES

Le droit d'accès aux ressources est personnel et incessible. Sa durée est limitée ; il cesse dès que la position de l'utilisateur ne le justifie plus.

Les moyens d'accès tangibles (clef, carte magnétique, ...) éventuellement remis à un utilisateur, sont personnels et incessibles. Il ne doit ni les prêter, ni les donner ni les vendre. Il doit les rendre en fin d'activité et signaler immédiatement leur vol ou disparition.

Outre le droit normal d'usage, l'étendue des ressources auxquelles l'utilisateur a accès peut être techniquement limitée en fonction de ses besoins réels et des contraintes imposées par le partage des ressources avec les autres utilisateurs.

L'utilisateur est responsable de l'utilisation des ressources informatiques (locales ou distantes) faite à partir de son compte. Cela implique qu'il prenne quelques précautions simples mais efficaces :

- choisir un mot de passe sûr (caractères + chiffres) et gardé secret,
- changer régulièrement son mot de passe, notamment après chaque démonstration en public,
- terminer proprement ses sessions et ne pas quitter son poste de travail en laissant une session active,
- prévenir les administrateurs de toute tentative de violation (même non réussie) de son compte,
- protéger ses fichiers, en particulier enlever les accès non indispensables,
- ne pas laisser traîner de support magnétique, optique ou autres (disquette, cartouche, cédérom,...).

Le droit d'accès peut être annulé avec ou sans préavis si le comportement d'un utilisateur contrevient gravement aux règles définies par la charte.

3. RESPECT DES OBLIGATIONS LÉGALES

Tout utilisateur interne ou externe est évidemment tenu de respecter les lois et règlements portant sur le traitement de l'information, notamment :

- la loi N°78-17 relative à l'informatique, aux fichiers et aux libertés du 6/1/78, modifiée par les lois N° 88-227 du 11/3/88 et No 94-548 du 1/7/94 (nouveau code pénal de 1994), qui traite des systèmes de traitement de l'information contenant des données nominatives sur les individus.
- la loi N° 85-660 relative aux droits d'auteur (logiciels) du 3/7/85 (titre 5 : protection contre la copie illicite de logiciels /cf code de la propriété intellectuelle), qui concerne les logiciels, les données informatiques, les données saisies ou numérisées à des fins d'incorporation dans un document. Il faut toujours garder à l'esprit que toute copie de logiciel protégé est interdite : une telle copie est pénalement assimilée à un vol.
- la loi N° 88-19 relative à la fraude informatique (loi Godfrain) du 5/1/88 (cf nouveau code pénal, art. 323-1 à 323-7) qui traite :
  - des accès ou maintien frauduleux dans un système informatique,
  - des atteintes volontaires au fonctionnement d'un système informatique,
  - des consultations non autorisées,
  - du détournement ou de l'altération de programmes ou données informatiques.
- les lois sur l'utilisation du cryptage (art. 28 de la loi N° 90-1170 du 29/12/90 modifié par l'article 17 de la loi N° 96-659 du 26 juillet 1997) qui prévoient que:
  - le cryptage à des fins d'authentification est sujet à déclaration préalable,
  - le cryptage des données est soumis à autorisation.

4. RESPECT DES OBLIGATIONS CONTRACTUELLES

Lorsque des logiciels ou des données fournis par un éditeur sont couverts par des droits de licence, les obligations contractuelles doivent être scrupuleusement suivies par l'utilisateur. Ceci concerne en particulier :

- l'interdiction des copies, telle qu'elle est prescrite par le droit général,
- les limitations d'usage à des fins d'enseignement ou non commerciales.

5. RÈGLES DE BONNE CONDUITE

5.1 RESPECT DE LA CONFIDENTIALITE DES INFORMATIONS

Les fichiers individuels ou collectifs sont privés, même s'ils sont physiquement accessibles : la possibilité matérielle de lire un fichier n'implique pas l'autorisation de le lire. Il ne faut donc tenter ni de lire ni de copier les fichiers d'un autre utilisateur ou groupe d'utilisateurs sans autorisation, ni d'intercepter des communications privées entre utilisateurs.

5.2 RESPECT DES INDIVIDUS

Chacun a le droit de travailler sans être dérangé : la liberté d'expression n'autorise en rien le harcèlement ou les insultes via forum, mail, téléphone, ou autre moyen de communication. La possibilité matérielle de modifier un fichier n'implique pas l'autorisation de le modifier (la destruction ou la modification de fichiers d'utilisateurs relève du vandalisme). Un utilisateur ne doit pas se voir limiter ou interdire l'accès aux ressources par un autre utilisateur.
La tentative d'usurpation d'identité est un délit.

5.3 RESPECT DES RESSOURCES PRIVEES

Certaines ressources (serveurs, imprimantes, ...) accessibles par le réseau ne sont pas publiques, mais appartiennent à un service particulier non disponible pour tous. Si les ressources physiquement protégées sont toujours privées, les ressources non physiquement protégées peuvent éventuellement être privées : il faut donc se renseigner avant toute utilisation.

Un environnement éducatif est naturellement ouvert : il ne faut pas en abuser. Les stations de travail et imprimantes privées nécessitent toujours une autorisation avant utilisation. Certains serveurs spécialisés peuvent comporter des restrictions d'accès.

Enfin, si certains fichiers du système d'exploitation (n'appartenant en propre à aucun utilisateur) restent lisibles à des fins d'enseignement, ils ne doivent en aucun cas être modifiés, ni même recopiés (la plupart des fichiers du système d'exploitation sont couverts par un droit de licence). Cela s'applique bien entendu à tous les serveurs accessibles par le réseau.

5.4 RESPECT DES RESSOURCES COMMUNES

Le partage des ressources par un nombre d'utilisateurs ayant des besoins souvent fort différents implique le respect de quelques règles.

5.4.1 Partage équitable des ressources communes

Espace disque : son utilisation doit être surveillée afin de réduire le gaspillage au minimum (nettoyage fréquent, compression, archivage, ...).

Système : les traitements gourmands en unité centrale doivent utiliser au mieux le traitement par lots et l'exécution aux heures creuses ; les sessions interactives multiples inactives sont proscrites.

Impression : éviter les longues impressions aux heures de pointe.

Seul le niveau utilisateur est autorisé sur un serveur commun ; un tel serveur ne peut servir à des enseignements ou manipulations expérimentales de programmation système ou réseau (développements appelant des fonctions internes du système, programmation de sockets, ...), ceci afin de maintenir l'intégrité du système et du réseau. L'installation de logiciels ou utilitaires, pouvant porter atteinte au fonctionnement des machines, n'est pas autorisée. C'est le cas notamment de tout logiciel provoquant une charge inappropriée de la machine, un dysfonctionnement, ou une modification de l'environnement standard.

5.4.2 Accès aux salles contenant le matériel informatique

Chaque utilisateur est tenu de respecter les règles d'accès ainsi que les notes affichées et les messages sur les écrans d'ordinateurs. Il ne faut pas dégrader le matériel en libre-service, modifier les systèmes d'exploitation ou changer la configuration d'utilisation ; il faut prévenir le personnel d'exploitation des problèmes rencontrés afin qu'ils soient corrigés.

5.4.3 Utilisation des réseaux

L'interconnectivité actuelle permet une grande convivialité dans l'utilisation des ressources académiques mondiales : cela nécessite des règles strictes de bonne conduite sous peine de se voir exclure de cette communauté. Les ressources ne doivent pas être utilisées pour se connecter sans autorisation sur des systèmes distants : possibilité matérielle de connexion ne signifie pas autorisation.

Les agissements suivants sont considérés comme des fautes graves :

- interrompre le fonctionnement normal du réseau ou d'un des systèmes connectés,
- accéder à des informations privées d'autres utilisateurs sur le réseau,
- modifier ou détruire des informations sur un des systèmes connectés,
- rendre nécessaire la mise en place de moyens humains ou techniques complémentaires pour contrôler les agissements d'un utilisateur sur le réseau.

5.4.4 Intégrité des systèmes informatiques

Le développement, l'installation ou la simple copie sur un serveur ou poste de travail individuel d'un programme ayant les objectifs ci-dessous sont strictement interdits :

- harcèlement d'un ou plusieurs autres utilisateurs,
- contournement de la sécurité,
- saturation des ressources,
- virus et cheval de Troie,
- contournement des protections des logiciels,
- écoute des réseaux (sniffers,...).

6. RESPONSABILITE DE L'ECOLE

L'utilisation des systèmes informatiques de l'Ecole implique l'adhésion à la présente charte. En conséquence, l'Ecole ne pourra être tenue responsable de toute détérioration d'informations du fait d'un utilisateur qui ne se serait pas conformé à ses dispositions. Cette responsabilité sera reportée sur l'auteur des troubles à titre personnel.

7. SANCTIONS

Le non-respect des règles de la présente charte, ainsi évidemment que des textes de lois et règlements en vigueur, peut conduire à des sanctions administratives ou pénales.

7.1 SANCTIONS ADMINISTRATIVES

Celles-ci seront prononcées par l'instance compétente pour la catégorie d'utilisateur fautif.

7.2 SANCTIONS PENALES

L'Ecole, et en particulier le directeur chargé de l'informatique et des télécommunications, est tenue par la loi de signaler toute violation constatée des lois et règlements. L'Ecole se réserve le droit d'engager des poursuites judiciaires pour sanctionner les violations particulièrement graves des règles d'usage de ses systèmes informatiques.