ACADÉMIE de MONTPELLIER
Institut Universitaire de Formation des Maîtres

Service Informatique
O. AGUSSOL

Rédacteur : O. Agussol – service informatique
Réf. : CharteIUFM_Montpellier_v1.doc
Date : Juin 2003

Charte de l'utilisateur pour l'usage de ressources informatiques et de services Internet

Objectif de la charte et domaine d'application

Ce texte est avant tout un code de déontologie. Il a pour objet de préciser la responsabilité des utilisateurs en accord avec la législation afin d'instaurer un usage correct des ressources informatiques et des services Internet, avec des règles minimales de courtoisie et de respect d'autrui.
La présente charte a pour objet d'informer tout utilisateur des ressources informatiques de l'IUFM de l'académie de Montpellier (ci après " l'IUFM ") des règles d'usage des moyens informatiques et de rappeler l'état actuel de la législation en matière de protection des logiciels et de fraude informatique.

Définitions

Le **Responsable de la Sécurité des Systèmes d'Information de l'IUFM** (R.S.S.I) et son suppléant sont deux personnes chargées par le Directeur de l'IUFM de la sécurité en matière d'informatique et de réseaux pour l'ensemble de l'IUFM.
Ce document utilise indifféremment les termes "**moyens informatiques**", "systèmes informatiques" ou "ressources informatiques". Les moyens informatiques de l'I.U.F.M. comprennent l'ensemble des serveurs, micro-ordinateurs et réseaux des secteurs pédagogiques, administratifs et techniques, y compris leurs logiciels. Ils englobent également tout logiciel ou matériel affecté au fonctionnement du réseau d'établissement.
Les règles et obligations définies dans cette charte s'appliquent à tout utilisateur des moyens informatiques de l'établissement et extérieurs accessibles via les réseaux informatiques de l'I.U.F.M..

On désigne par `` **services Internet** '' la mise à disposition, par des serveurs locaux ou distants de moyens d'échanges ou d'informations diverses : Web, messagerie, forums ...
On appelle "**utilisateur**" toute personne physique, quelque soit son statut : étudiant, enseignant, chercheur, ingénieur, technicien, administratif, personnel temporaire, stagiaire, ... appelée à utiliser les ressources informatiques de l'établissement
les ressources informatiques et les réseaux de l'établissement.

C**ONDITIONS D'ACCES AUX RESSOURCES INFORMATIQUES ET AUX RESEAUX**

L'utilisation des moyens informatiques et des réseaux de l'IUFM doit être limitée à des activités administratives, de recherche, d'enseignement et de formation, de gestion ou de vie de l'établissement.
L'utilisateur ne peut pas connecter un équipement informatique aux ressources informatiques et aux réseaux de l'établissement sans autorisation préalable.
L'utilisateur doit respecter les modalités de raccordement des matériels aux réseaux de communication telles qu'elles lui sont précisées par le responsable des moyens informatiques. Ces raccordements ne pourront pas être modifiés sans autorisation préalable.
L'utilisateur est responsable de l'utilisation des ressources informatiques (locales ou distantes) effectuée à partir de son droit d'accès.
Le droit d'accès est temporaire; il est retiré dans les cas suivants :
- la fonction de l'utilisateur ne le justifie plus ;
- le non-respect du présent règlement.
Sauf autorisation écrite du Directeur de l'IUFM ou du responsable de service, les moyens informatiques ne peuvent être utilisés pour d'autres activités n'entrant pas dans le champ des missions de l'IUFM. Conformément à la législation en vigueur, l'accès aux ressources informatiques de l'IUFM ainsi qu'à Internet à travers son réseau ne sont autorisés que dans le cadre exclusif de l'activité professionnelle.
L'utilisation de ressources informatiques et l'usage des services Internet ainsi que du réseau pour y accéder ne sont autorisés que dans le cadre exclusif de l'activité professionnelle des utilisateurs conformément à la législation en vigueur.
L'activité professionnelle est celle prévue par les statuts du GIP RENATER (Groupement d'Intérêts Public, REseau NAtional de télécommunications pour la Technologie, l'Enseignement et la Recherche) auquel est lié l'IUFM, à savoir : les activités de recherches, d'enseignements, de développements techniques, de transferts de technologies, de diffusion d'informations scientifiques, techniques et culturelles, d'expérimentations de nouveaux services présentant un caractère d'innovation technique, mais également toute activité administrative et de gestion découlant ou accompagnant les activités.

Usage des services Internet (web, messagerie, forum...)

L'utilisateur doit faire usage des services Internet dans le cadre exclusif de ses activités professionnelles et dans le respect de principes généraux et des règles propres aux divers sites qui les proposent ainsi que dans le respect de la législation en vigueur (Notamment la Charte RENATER).
En particulier :
- il ne doit pas se connecter ou essayer de se connecter sur un serveur autrement que par les dispositions prévues par ce serveur ou sans y être autorisé par les responsables habilités ;

- il ne doit pas se livrer à des actions mettant sciemment en péril la sécurité ou le bon fonctionnement des serveurs auxquels il accède ;
- il ne doit pas usurper l'identité d'une autre personne ;
- il ne doit pas intercepter de communications entre tiers et il a l'obligation de s'abstenir de toute ingérence dans la transmission des messages en vertu du secret des correspondances privées ;
- il ne doit pas utiliser ces services pour proposer ou rendre accessible aux tiers des données et informations confidentielles ou contraires à la législation en vigueur ;
- il ne doit pas déposer des documents sur un serveur sauf si celui-ci le permet ou sans y être autorisé par les responsables habilités ;
- il doit faire preuve de la plus grande correction à l'égard de ses interlocuteurs dans les échanges électroniques par courrier, forums de discussions...
- il n'émettra pas d'opinions personnelles étrangères à son activité professionnelle susceptibles de porter préjudice à l'IUFM;
- il doit s'imposer le respect des lois et notamment celles relatives aux publications à caractère illicite, injurieux, raciste, pornographique, diffamatoire.

L'entité, et plus généralement l'IUFM, ne pourra être tenue pour responsable des détériorations d'informations ou des infractions commises par un utilisateur qui ne se sera pas conformé à ces règles.

Préservation de l'intégrité des systèmes informatiques

RESPECT DU CARACTERE CONFIDENTIEL DES INFORMATIONS

L'utilisateur ne doit pas tenter de lire ou de copier les fichiers d'un autre utilisateur sans son autorisation.

Les informations contenues dans les fichiers d'un utilisateur sont privées même si les fichiers sont " physiquement " accessibles.

L'utilisateur doit s'abstenir de toute tentative d'interception de communications privées entre utilisateurs.

La création de tout fichier contenant des informations nominatives doit faire l'objet d'une demande préalable auprès de la Commission Nationale de l'Informatique et des Libertés (CNIL).

Les fichiers en la possession des utilisateurs doivent être considérés comme privés et confidentiels, qu'ils soient ou non accessibles à d'autres utilisateurs. Le droit de lecture ou de modification d'un fichier ne peut être exercé qu'après accord explicite de son propriétaire.

En particulier, il est interdit de prendre connaissance d'informations détenues par d'autres utilisateurs sans leur accord. Cette règle s'applique également aux conversations privées de type messagerie électronique.

Les utilisateurs sont tenus à l'obligation de réserve sur toute information relative au fonctionnement interne de l'établissement qu'ils auraient pu obtenir en utilisant les ressources informatiques.

Si, dans l'accomplissement de son travail, l'utilisateur est amené à constituer des fichiers dont le contenu relève de la loi Informatique et Libertés, il devra auparavant se rapprocher du responsable de site qui sollicitera du service central la saisine de la CNIL. Il ne pourra en tout état de cause constituer ces fichiers avant d'en avoir reçu l'autorisation. Il est rappelé que cette

autorisation n'est valable que pour le traitement défini dans la demande et non pour le fichier lui-même.

L'utilisateur doit s'abstenir de toute tentative de s'approprier ou de déchiffrer le mot de passe d'un utilisateur, de modifier, copier ou détruire des fichiers d'un autre utilisateur, et de limiter ou d'interdire l'accès aux systèmes informatiques d'un utilisateur autorisé.

Article 4 - RESPECT DES DROITS DE PROPRIETE

Il est interdit à tout utilisateur de faire des copies de logiciels commerciaux pour quelque usage que ce soit. Les copies de sauvegarde sont la seule exception.
Tout utilisateur doit de plus se conformer aux prescriptions d'utilisation définies par l'auteur et/ou le fournisseur d'un logiciel. Il est strictement interdit d'installer un logiciel sur un système sans s'être assuré préalablement que les droits de licence le permettent.

RESPECT DES PRINCIPES DE FONCTIONNEMENT DES SYSTEMES INFORMATIQUES

L'utilisateur s'engage à ne pas apporter volontairement des perturbations au bon fonctionnement des systèmes informatiques et des réseaux que ce soit par des manipulations anormales du matériel, ou par l'introduction de logiciels parasites connus sous le nom générique de virus, chevaux de Troie, bombes logiques, logiciels d'écoute réseau ...

En particulier, tout utilisateur devra se garder strictement :

- d'interrompre le fonctionnement du réseau ou des systèmes connectés au réseau (manipulations anormales, introduction de virus, ...);
- d'essayer de se connecter frauduleusement à tout système d’information;
- d'utiliser le login d'un autre utilisateur
- d'accéder à des informations appartenant à d’autres utilisateurs du réseau, sans leur autorisation ;
- de modifier ou détruire des informations appartenant à d'autres utilisateurs et ceci sans leur autorisation;
- de porter atteinte à un autre utilisateur, notamment par l'intermédiaire de messages, textes ou images provocants ;
- de masquer sa véritable identité;
- de développer des outils mettant sciemment en cause l'intégrité des systèmes ;
- de nuire à l'image de marque de l’établissement.

La sécurité est l'affaire de tous, chaque utilisateur de l'informatique et du réseau d'établissement doit y contribuer à son niveau, et mettre en application un certain nombre de règles de bon sens et des recommandations fournies par les responsables de site.

Parmi les règles de bon usage:

- user raisonnablement de toutes les ressources partagées (puissance de calcul, espace disque, bande passante du réseau, ...) ;

- ne jamais quitter son poste de travail en laissant une session ouverte ;
- protéger ses fichiers, avec l'aide éventuelle des responsables de site; l'utilisateur est responsable des droits qu'il accorde à des tiers ;
- choisir des mots de passe sûrs. Ces mots de passe doivent être tenus secrets, ne pas être écrits sur un document papier, ne jamais être communiqués à un tiers et être changés régulièrement ;
- sauvegarder régulièrement ses fichiers et éventuellement en restreindre l'accès avec l'aide du responsable de site.

Respect d'un comportement correct

L'utilisateur ne doit pas utiliser les systèmes informatiques pour harceler d'autres utilisateurs par des communications non souhaitées par les tiers ou pour afficher/diffuser des informations illégales.
Il est rappelé que des lois plus générales s'appliquent pour des informations ou messages :
- à caractère injurieux,
- à caractère pornographique,
- à caractère diffamatoire,
- d'incitation au racisme,
- etc ....

DROITS ET DEVOIRS DE L'ADMINISTRATEUR D'UNE RESSOURCE INFORMATIQUE

Pour des nécessités de sécurité, de maintenance et de gestion technique, l'utilisation des ressources matérielles ou logicielles ainsi que les échanges via le réseau peuvent, sous le contrôle du R.S.S.I, être analysés et contrôlés dans le respect de la législation applicable et notamment de la loi relative à l'informatique, aux fichiers et aux libertés.

Tout administrateur système et/ou réseau a le droit :

- d'être informé des implications légales de son travail, en particulier des risques qu'il court dans le cas où un utilisateur du système dont il a la charge commet une action répréhensible,
- d'accéder, sur les systèmes qu'il administre, aux informations privatives à des fins de diagnostic et d'administration du système, en respectant scrupuleusement la confidentialité de ces informations, en s'efforçant tant que la situation ne l'exige pas de ne pas les altérer.
- d'établir des procédures de surveillance de toutes les tâches exécutées sur la machine, afin de déceler les violations ou les tentatives de violation de la présente charte, sous l'autorité de son responsable fonctionnel et en relation avec le correspondant sécurité informatique,
- de prendre des mesures conservatoires si l'urgence l'impose, sans préjuger des sanctions résultants des infractions à la présente charte qui sont de la responsabilité des responsables

Tout administrateur système et/ou réseau a le devoir :

- d'informer les utilisateurs sur l'étendue des pouvoirs dont lui-même dispose techniquement de par sa fonction,

- d'informer les utilisateurs et de les sensibiliser aux problèmes de sécurité informatique inhérents au système,
- de leur faire connaître les règles de sécurité à respecter,
- de saisir l'autorité hiérarchique des manquements graves résultant du non respect de cette charte pouvant déclencher des procédures disciplinaires ou pénales.

COLLECTE ET UTILISATIONS D'INFORMATION

Informations collectées

- Lors de la connexion de l'utilisateur aux ressources informatiques de l'IUFM, celui-ci est amené à collecter des informations concernant la date et heure de connexion et de déconnexion au réseau de l'IUFM, l'envoi et la réception de messages et le suivi de la navigation Internet afin de disposer des noms de domaines des sites visités par l'utilisateur.
Ces informations seront détruites au bout d'un an.

Utilisation aux fins de gestion et d'amélioration

- La principale finalité de la collecte des informations visées ci-dessus est la fourniture, au profit de l'Utilisateur, d'un service optimal. Cette optimisation passe par le suivi des flux de données voire le contrôle d'usage des ressources mises à disposition et la vérification qu'il correspond aux missions de l'IUFM. Toutefois ce contrôle ne peut être exécuté que sur demande expresse du Directeur de l'IUFM

Transmission des données à des tiers

- L'Utilisateur est informé que l'IUFM peut être amené à communiquer, à des autorités publiques ou judiciaires, des informations concernant l'utilisation des ressources mises à disposition.

SANCTIONS APPLICABLES

Des dispositions réglementaires définissent les droits et obligations des personnes utilisant les moyens informatiques.
Tout utilisateur n'ayant pas respecté ces dispositions se voit retirer ses accès aux ressources informatiques de l'IUFM et peut être poursuivi pénalement. De même le non respect de la charte est également passible de sanctions administratives proportionnelles aux fautes commises pouvant se traduire par la demande de sanctions disciplinaires aux autorités compétentes.
Les sanctions pénales, administratives et disciplinaires ne sont pas exclusives les unes des autres.
Seul le Directeur de l'IUFM est habilité à saisir le Procureur de la République, dans le cadre de l'autorisation qui lui a été accordée par le Conseil d'administration.

L'évolution des techniques électroniques et informatiques a conduit le législateur à définir des sanctions à la mesure du risque que peut faire courir aux libertés individuelles et au Droit l'usage incontrôlé des fichiers ou des traitements informatiques. Cette charte est portée à la connaissance de l'ensemble du personnel et s'impose à tous.

Rappel de quelques textes de loi

Protection des personnes :

Loi du 6 janvier 1978, modifiée, sur l'informatique et les libertés. Cette loi a pour objet de protéger les libertés individuelles susceptibles d'être menacées par l'utilisation de l'informatique. Elle définit les droits des personnes et les obligations des responsables de fichiers.

Loi 92-684 du 22 juillet 1992, modifiée. (déclaration préalable à la création de tout fichier contenant des informations nominatives)

Article 226-24 du Nouveau Code Pénal (NCP) responsabilité des personnes morales des infractions aux dispositions de la loi sur les atteintes à la personnalité.

Convention Européenne du 28/01/1981

Protection des logiciels

Lois du 3 juillet 1985 et du 1er juillet 1992 sur la protection des logiciels. Ces lois protègent les droits d'auteur. Elles interdisent en particulier à l'utilisateur d'un logiciel toute reproduction autre que l'établissement d'une copie de sauvegarde;

Loi du 10 mai 1994 modifiant la loi du 1er juillet 1992 relative au code de Propriété intellectuelle.

Directive Européenne du 21/12/1988 (harmonisation de la protection juridique des logiciels)

Protection des secrets par nature
Art 410-1 et 411-6 secrets économiques et industriels
Art 432-9 al et 226-15 al1 secret des correspondances (écrites, transmises par voie de télécommunications)

Accès ou maintien frauduleux dans un système informatique
Loi du 5 janvier 1988 relative à la fraude informatique
C'est la loi la plus importante et la plus astreignante puisqu'elle définit les peines encourues par les personnes portant atteinte aux systèmes de données.

Art 323-1 et suivant du NCP : 1 à 2 ans d'emprisonnement et 100000 à 200000 Fr d'amende (dans le cas de modification du système)

Art 323-5 peines complémentaires