



CHARTRE DE L'IUFM DE LA REUNION POUR LE BON USAGE DE L'INFORMATIQUE ET DES RESEAUX

1. PRINCIPES GENERAUX

1.1 Objet - La présente charte a pour objet d'informer tout utilisateur des ressources informatiques de l'Institut Universitaire de Formation des Maîtres de La Réunion (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.

Ce document utilise indifféremment les termes "moyens informatiques", "systèmes informatiques" ou "ressources informatiques". Les moyens informatiques de l'I.U.F.M. de La Réunion 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. de La Réunion.

On appelle "utilisateur" toute personne physique, quel que soit son statut : étudiant, enseignant, chercheur, ingénieur, technicien, administratif, personnel temporaire, stagiaire,... appelée à utiliser les ressources informatiques de l'établissement.

1.2 Acceptation de la Charte - La charte est remise à chaque utilisateur qui doit en prendre connaissance et retourner le feuillet d'acceptation signé.

2. REGLES D'ACCES

Le droit d'accès d'un utilisateur au système d'information est soumis à autorisation. Il est personnel et incessible ; il est supprimé lorsque la justification de cet accès disparaît. Ce droit est en outre limité à des activités conformes aux missions de l'établissement (recherche, enseignement, administration).

Sauf autorisation écrite du chef d'établissement 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'accès au réseau est soumis à une procédure d'authentification qui se traduit par l'attribution d'un compte d'accès individuel (login et mot de passe). Le mot de passe fourni à l'utilisateur est, à l'image du login, personnel, confidentiel et incessible. Chaque utilisateur étant responsable de l'utilisation des ressources informatiques qui est faite avec son identifiant, il ne doit donc pas se servir sauf disposition particulière d'un autre login que celui qui lui a été attribué.

Les postes de travail individuels ne doivent pas être utilisés sans la permission des personnes à qui ils sont affectés ou d'un responsable hiérarchique.

Tout utilisateur devra respecter les modalités de raccordement des matériels au réseau de l'établissement. Ces modalités sont établies par le service informatique de l'IUFM.

Tout ordinateur relevant des structures pédagogiques ou des services administratifs devant être connecté au réseau devra être déclaré au service informatique. Ce dernier doit en particulier s'assurer que les règles de sécurité et de confidentialité sont bien respectées.

3. CONFIDENTIALITE (RESPECT DE LA / CONDITIONS DE)

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 service informatique qui sollicitera 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.

4. RESPECT DU DROIT 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.

5. LES PRINCIPES A RESPECTER

Tout utilisateur est responsable de l'utilisation qu'il fait des ressources informatiques et s'engage à ne pas effectuer des opérations qui pourraient avoir des conséquences néfastes sur le fonctionnement du réseau, sur l'intégrité de l'outil informatique, et sur les relations internes et externes de l'établissement.

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 compte d'accès 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 le service informatique. Parmi les règles de bon usage :

- ? ne jamais quitter son poste de travail en laissant une session ouverte
- ? user raisonnablement de toutes les ressources partagées (puissance de calcul, espace disque, bande passante du réseau, ...)
- ? protéger ses fichiers, avec l'aide éventuelle du service informatique ; 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 service informatique
- ? signaler au service informatique tout fonctionnement anormal pouvant relever d'une attaque d'un virus informatique

6. COLLECTE ET UTILISATION D'INFORMATIONS

6.1 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.

Les utilisateurs sont informés que l'administrateur du réseau a accès à l'ensemble de toutes les données qui sont susceptibles de circuler sur le réseau de l'IUFM. L'administrateur s'engage à ne pas divulguer ces données sauf cas prévu à l'article 6.3 suivant.

6.2 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

6.3 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.

7. 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.

8. RESPONSABILITE ET OBLIGATIONS DE L'IUFM

L'IUFM est lui-même soumis aux règles de bonne utilisation des moyens informatiques, et se doit de faire respecter les règles définies dans ce document.

L'IUFM ne pourra être tenu pour responsable de détérioration d'informations du fait d'un utilisateur ne s'étant pas conformé à l'engagement qu'il a signé.

9. ENGAGEMENT PERSONNEL

Je soussigné, nom : prénom :

qualité :

utilisateur des moyens informatiques et réseaux de l'IUFM de La Réunion, déclare avoir pris connaissance de la présente charte et m'engage à me conformer strictement au bon usage de l'informatique et des réseaux.

A, le

signature précédée de la mention "lu et approuvé"

(à compléter et à remettre au service informatique)

Rappel de quelques textes de lois

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 F d'amende (dans le cas de modification du système)
- ? Art 323-5 peines complémentaires