CHARTE DU BON USAGE DES MOYENS INFORMATIQUES ET DU RESEAU DE L'UNIVERSITE PAUL SABATIER

La présente charte a pour objet, de définir les règles d'utilisation des moyens informatiques au sein de l'établissement et de rappeler à chacun des utilisateurs ses responsabilités.

Texte approuvé par le Conseil des Etudes et de la Vie Universitaire de l'Université le : 17 février 1999

Texte approuvé par le Conseil Scientifique de l'Université le : 4 mars 1999

1 Domaine d’application

Les règles et obligations énoncées ci-dessous s'appliquent à tout utilisateur des ressources informatiques de l'Université : étudiant, enseignant, enseignant-chercheur, chercheur, personnel administratif ou technique, ouvrier et de service. Ces ressources comprennent les serveurs, les stations de travail et micro-ordinateurs et leurs périphériques, situés dans les services administratifs, les locaux d’enseignement, les laboratoires de l'Université et tout autre local de l’Université disposant de tels matériels.

Les installations de l'Université permettant de se connecter ou de dialoguer avec des sites informatiques dans le monde entier, les règles définies par la présente charte s'étendent également à l'utilisation des ressources des réseaux extérieurs, accessibles par l'intermédiaire de réseaux d’interconnexion comme RéMiP, RENATER et Internet.

Le non-respect des règles de bonne conduite énoncées dans le présent document engage la responsabilité personnelle de l'utilisateur.

L'établissement, par sa signature de la charte du réseau RENATER, est lui-même soumis aux règles de bonne utilisation des moyens informatiques et, à ce titre, se doit de faire respecter les règles déontologiques et la loi.

2 Respect de la déontologie informatique

2.1 Principes fondamentaux

Tout utilisateur est responsable de l'usage qu'il fait des ressources informatiques. Il doit particulièrement veiller à user raisonnablement de toutes les ressources partagées auxquelles il accède (puissance de calcul, espace disque, bande passante du réseau, ...).

Tout utilisateur s'engage à respecter les règles de la déontologie informatique et notamment à ne pas effectuer des opérations ayant pour but :

- de masquer sa véritable identité ;
- d'usurper l'identité d'autrui ;
- de s'approprier le mot de passe d'un autre utilisateur ;
- de mettre en place un programme pour contourner les procédures établies dans le but d’augmenter le niveau de sécurité des systèmes ;
- d’utiliser ou de développer des programmes mettant sciemment en cause l'intégrité des systèmes informatiques ;
- d'installer et d'utiliser un logiciel à des fins non conformes aux missions de l'Université ;
- de ne pas respecter les règles d'accès aux salles contenant le matériel informatique ;
- d'utiliser des comptes autres que ceux auxquels il a légitimement accès ;
- d'utiliser un poste de travail ou tout autre ressource informatique sans une autorisation explicite de la personne à qui elle est attribuée ;
- d'accéder aux données d'autrui sans l'accord exprès des détenteurs, même lorsque ces données ne sont pas explicitement protégées.

L'usage des supports de communication électronique (courrier, forums de discussion, documents accessibles par le WEB, ...) doit se faire dans le respect des règles suivantes :

- ne pas porter atteinte à l'intégrité d'un autre utilisateur ou à sa sensibilité, notamment par l'intermédiaire de messages, textes ou images provocants,
- préciser si l’expression est faite à titre personnel ou au nom de l'établissement, d’une de ses composantes et ce, particulièrement dans toute communication à diffusion publique.

2.2 Principes complémentaires

Un certain nombre de textes de lois viennent préciser ou compléter les principes de la déontologie informatique déjà présentés.

2.2.1 La protection des libertés individuelles

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).

Le nouveau code pénal définit dans ce domaine les délits qui peuvent être constitués, non pas seulement s'il y a intention coupable, mais dès lors qu'il y a négligence, imprudence ou même incompétence professionnelle et énonce les sanctions afférentes dans une section intitulée « des atteintes aux droits des personnes résultant des fichiers ou des traitements informatiques » (articles 226-16 à 226-22).

2.2.2 Le respect du droit de propriété

La législation interdit à tout utilisateur de faire des copies de logiciels commerciaux pour quelque usage que ce soit. Les copies de sauvegarde sont les seules exceptions.

La copie d'un logiciel constitue le délit de contrefaçon sanctionné pénalement (code de la propriété intellectuelle). 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.

2.2.3 Le respect de l'intégrité d'un système informatique

L'utilisateur s'engage à ne pas effectuer des opérations pouvant nuire au bon 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 font l'objet des articles 323-3 et 323-4 du nouveau code pénal.

Il est important de noter que la simple tentative ainsi que la participation à une entente établie en vue de la préparation d’une infraction est punie des peines prévues pour l’infraction elle-même.

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).

2.2.4 Le respect du secret de la correspondance

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

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 » . Le téléphone, le télécopieur et les liaisons informatiques et télématiques sont donc concernés par ce texte.

De lourdes sanctions pénales frappent celui qui porte atteinte au secret de la correspondance (articles 226-15 et 432-9 du nouveau code pénal).

2.3 Autres obligations légales

Certaines dispositions légales, ayant une application dans le cadre de l'utilisation des ressources informatiques, sont présentées ici.

2.3.1 Le dépôt légal

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 20juin 1992).

2.3.2 L'usage de la cryptographie

La cryptographie est définie par l'article 28-1 de la loi numéro 90-1170 du 29 décembre 1990 : « On entend par prestation de cryptographie, toutes prestations 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 cryptographie, 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 des télécommunications doit respecter les procédures prévues par la loi, d'autorisation ou d'agrément préalable, sous peine de sanctions pénales.

2.3.3 Contenu des informations

Comme sur d'autres médias, 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 (actes réprimés par les lois **numéro 90-615du 13 juillet 1990 et numéro 92-1336 du 16 décembre 1992).**

3 Accès aux ressources informatiques

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 de l'information scientifique et technique, la coopération internationale (article 4 de la loi numéro 84- 52 du 26 janvier 1984) et la vie universitaire. Par ailleurs, l'étendue des ressources informatiques auxquelles l'utilisateur a accès peut être limitée en fonctions des besoins réels et des contraintes imposées par le partage de ces ressources avec les autres utilisateurs.

Le droit d'accès est temporaire, il est retiré si la qualité de l'utilisateur ne le justifie plus. Il peut également être retiré, par mesure conservatoire du Président de l'Université, si le comportement d'un utilisateur n'est plus compatible avec les règles énoncées dans la présente charte.

Dans certains cas, un compte personnel peut être attribué. Ce compte est strictement personnel. Chaque utilisateur est responsable de l'utilisation qui en est faite. Nul n'est autorisé à utiliser le compte d'autrui.

Le mot de passe constitue la clé personnelle d'utilisation du compte et par conséquent ne doit être communiqué à qui que ce soit (y compris à un administrateur).

4 Droits et devoirs

4.1 Des utilisateurs

- La sécurité est l'affaire de tous, chaque utilisateur de l'informatique et du réseau d'établissement doit y contribuer en suivant ces quelques règles :
- Ne pas masquer sa véritable identité ;
- Ne pas usurper l'identité d'autrui ;
- Choisir un mot de passe sûr (il ne doit correspondre ni à un mot, ni à un nom propre et ce, dans quelque langue que ce soit) et gardé secret ;
- Ne jamais donner son mot de passe à un tiers (y compris un administrateur système) ;
- Ne pas afficher de mot de passe, même si le poste de travail est partagé par plusieurs personnes ;
- Changer régulièrement de mot de passe ;
- Ne pas quitter son poste de travail en laissant une session en cours ;
- Ne jamais prêter son compte ;
- Signaler aux administrateurs systèmes toute violation, tentative de violation ou toute violation suspectée d'un système informatique et, de façon générale, toute anomalie constatée (mauvaise gestion des protections, faille système, logiciel suspect,...) pouvant nuire au bon niveau de sécurité du système.

4.2 Des administrateurs des systèmes informatiques

Les administrateurs des différents systèmes 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, les administrateurs des systèmes peuvent être amenés (avec l'autorisation du responsable de service, de laboratoire, de composante ou d'enseignement) à examiner le contenu de fichiers ou boîtes aux lettres, de façon à obtenir suffisamment d'informations pour pallier les incidents de fonctionnement ou s'il y a lieu, de pouvoir déterminer si un utilisateur ne respecte pas la politique d'utilisation des ressources informatiques de l'établissement décrite dans ce document.

Les administrateurs de systèmes ont l'obligation de préserver la confidentialité des informations privées qu'ils sont amenés à connaître dans ce cadre.

Les utilisateurs peuvent demander l'aide des administrateurs systèmes pour faire respecter leurs droits.

5 Sanctions

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 systèmes qui peuvent surveiller en détail des sessions de travail d'un utilisateur s'il existe un soupçon de non-respect de la charte ;

Leur compte peut être fermé, sur décision du responsable administratif du compte ou du Président de l'Université ;

Ils peuvent être traduits devant la Section Disciplinaire du Conseil d'Administration de l'Université en ce qui concerne les enseignants-chercheurs et les étudiants et devant le Conseil de Discipline de leur corps respectif en ce qui concerne les personnels administratifs et techniques, ouvriers et de service ;

Ils peuvent faire l'objet de poursuites pénales engagées à la demande du Président de l'Université.