

Le texte de la charte du bon usage de l'informatique

1. INTRODUCTION

1.1. La notion d'utilisateur...

On appelle << Utilisateur >> toute personne, quelque soit son statut : étudiant, enseignant, chercheur, technicien, administratif, personnel temporaire, stagiaire,... appelée à utiliser les ressources informatiques et réseaux de l'établissement.

1.2. Facilités apportées par la technique et effets induits

Pour quelques centaines de francs un ordinateur personnel devient un point d'entrée sur le réseau.

L'utilisateur isolé n'existe plus, il peut de chez lui accéder à son courrier électronique et à une multitude de services.

Toute technique qui se développe engendre dans son sillage, un lot de phénomènes pervers.

L'Informatique et ses applications n'échappent pas à cette constatation.

Les délits informatiques existent, ils sont de plus en plus nombreux, il ne s'agit pas ici de fournir une liste exhaustive, mais de donner quelques exemples parmi les plus fréquents.

Nous distinguerons entre délits liés à l'utilisation du réseau et délits relatifs à des ordinateurs travaillant localement.

1.2.1. Délits liés à l'utilisation du réseau :

- l'intrusion sur Ordinateur à travers un Réseau
- l'utilisation << détournée >> des ressources informatiques mises à disposition
- l'emprunt de l'identité d'un tiers
- l'utilisation d'une identité alors que l'on a perdu sa qualité d'utilisateur

1.2.2. Délits relatifs à la bureautique et à des ordinateurs travaillant localement

- la copie illicite de logiciel
- l'utilisation << détournée >> des ressources informatiques mises à disposition
- l'utilisation << par tiers non autorisé >> des ressources informatiques de l'établissement
- l'utilisation de logiciel non expressément autorisé

1.3. Remarques Préliminaires

* Toute personne << travaillant ou étudiant >> dans l'établissement est un utilisateur potentiel des moyens ou ressources informatiques de l'établissement.

* Tout utilisateur des moyens ou ressources informatiques de l'établissement a le devoir de respecter les règles de l'établissement.

* Ce respect des règles est la contrepartie obligée de la liberté d'utilisation et de communication qui est traditionnellement de mise dans tout établissement relevant de l'Enseignement Supérieur et la Recherche.

* La Charte de Bon Usage de l'Informatique et des Réseaux est un recueil des règles déontologiques qu'il convient de respecter scrupuleusement. Elle a pour objectif d'informer l'utilisateur et de l'avertir des risques qu'il encourt.

* Le non-respect de la Charte de Bon Usage de l'Informatique et des Réseaux, engage la responsabilité personnelle de l'utilisateur, imprudent, inconscient, irresponsable et peut nuire directement ou indirectement à tout ou partie de notre établissement.

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

* Les risques existent dans notre Etablissement, la sécurité passe par le respect des règles et la vigilance de chacun.

* Face aux risques, une pédagogie permanente s'impose, elle concerne tout responsable et tout personnel.

" Nul n'est censé ignorer la loi "

1.4. Graduation des sanctions

Qui dit << délits >>, dit << sanctions >>. Il est naturel que le non-respect des règles déontologiques se traduise par des sanctions.

Il existe une graduation des sanctions liées à la << gravité >> du délit par rapport aux règles de l'établissement. Il faut distinguer entre sanctions administratives et sanctions pénales : les unes n'étant pas exclusives des autres.

Seul, le Président de l'Université, en sa qualité de Chef de l'établissement, est habilité à saisir le Procureur de la République.

2. L'UTILISATION DU RÉSEAU

2.1. La DSII maître d'oeuvre

La DSII offre à l'ensemble des utilisateurs de l'Université de Provence des accès aux réseaux de campus, régional (R3T2) national (RENATER).

2.1.1. Qui est Utilisateur du réseau ?

Toute personne de l'Université de Provence autorisée à laquelle peut être attachée le triplet suivant :

- un compte sur une machine de la DSII ou d'un laboratoire, service ou formation installé sur l'un des campus de l'université.
- un mot de passe.
- une durée pendant laquelle elle a accès aux ressources informatiques de l'établissement.

2.1.2. Avertissements

* Tout utilisateur est responsable de l'utilisation qu'il fait des ressources informatiques mises à sa disposition par l'établissement.

* La DSII se réserve le droit de suspendre à tout moment l'accès au réseau pour inobservances de la part de l'utilisateur des règles de bon usage.

2.2. L'Université de Provence et le Respect de la Loi

* L'Université de Provence, consommatrice d'Informatique, utilisatrice des réseaux et productrice, notamment, de données scientifiques, n'échappe pas aux risques potentiels et se doit de faire respecter les lois en la matière.

* Le réseau de l'Université de Provence permettant la connexion et le dialogue notamment avec l'ensemble des organismes de l'Enseignement Supérieur et de la Recherche et le reste du monde, les accès inter-sites doivent se faire dans le strict respect des règles de bon usage et conformément à la législation en vigueur relative aux atteintes des systèmes de traitement automatisé de données. (Article 323-1 et suivants du Nouveau Code Pénal version du 1 mars 1994 relatifs à l'intrusion non autorisée dans un système)

* Toute tentative de nuire ou de mettre en péril sciemment d'autres sites, depuis des << machines >> connectées au réseau de l'université est passible de sanctions administratives et pénales.

* L'Université de Provence pour faire respecter les règles de bon usage de l'Informatique et des Réseaux dispose de façon complémentaire et non exclusive des règles administratives en usages en la matière et de l'arsenal juridique.

2.3. La Loi

2.3.1. La protection des Personnes : loi 92-684 du 22 juillet 1992

(Déclaration préalable à la création de tout fichier contenant des informations nominatives)

Article 226-24 du NCP* responsabilité des personnes morales des infractions aux dispositions de la loi sur les atteintes à la personnalité.

2.3.2. L'accès ou le maintien frauduleux dans un système informatique

Article 323-1 et suivants du NCP : 1 à 2 ans d'emprisonnement et 100 000 à 200 000 Fr. d'amende (max. dans le cas de modification du système)

Art 323-5 peines complémentaires (interdiction d'exercer dans la fonction publique ou certaine activité professionnelle...)

2.3.3. La Protection des secrets par nature

Art410-1 et 411-6 secrets économiques et industriels.

Art432-9 al 1 et 226-15 al 1 secrets des correspondances (écrites, transmises par voie de télécommunications)

* NCP Nouveau Code Pénal

3. L'UTILISATION DE MOYENS INFORMATIQUES & BUREAUTIQUES

Il s'agit d'essayer de traiter dans ce chapitre les risques liés à l'utilisation croissante et généralisée des moyens informatiques & bureautiques. Parmi les risques les plus fréquents relevés, il faut citer :

3.1. Risques les plus fréquents :

3.1.1. Le vol ou la duplication d'un support magnétique.

Ce risque est particulier aux machines faisant du traitement de texte, la recopie des fichiers et la duplication des disquettes étant simple et rapide.

3.1.2. Le vol ou la lecture illicite d'un document.

L'absence de comptage du nombre d'exemplaires produits ou reproduits augmente ce risque de façon sensible.

3.1.3. La lecture d'informations sur l'écran de visualisation.

Un document ne doit pas rester affiché sur l'écran de visualisation après exploitation. L'accès des locaux doit être contrôlé.

3.1.4. Le Virus informatique

De quoi s'agit-il ? d'une fonctionnalité cachée d'un logiciel, qui, lors de l'exécution de celui-ci, a la propriété de se reproduire de manière discrète dans d'autres programmes de la machine, allant jusqu'à détruire données et programmes ou encore à mettre la machine en panne. Le virus est implanté à l'intérieur d'un programme anodin appelé " vecteur ", c'est l'exécution de ce " vecteur " qui engendre le processus de prolifération.

3.1.4.1. Virus " Concepteur de logiciel "

Devant la multiplication des copies, autre que la copie de sécurité autorisée, certains concepteurs ont eu l'idée de "protéger" leur produit logiciel en " inoculant " à l'intérieur un virus qui se propage lorsque le nombre de copies est supérieur à un nombre déterminé, deux par exemple. La copie est faite, mais le logiciel copié va détruire les fichiers lors de la première utilisation. Cette protection constructeur a pour effet de lutter contre les copies illicites, donc l'usage relève du ... recel.

3.1.4.2. Virus de type ver

Ce type de virus se << nide >> en mémoire et à chaque appel d'une séquence particulière a pour effet de faire croître le programme jusqu'à ce qu'il ne reste plus de place pour exécuter la moindre instruction.

3.1.4.3. Remarque

Nombre de programmes de jeux, de disquettes << offertes >> dans des revues constituent d'excellents << porteurs sains >> de virus.

3.1.5. Système de protection de micro-ordinateurs

* par mot de passe et accès à tout ou partie des " dossiers " ou de l'espace de travail.

* par carte magnétique de type badge.

3.2. La loi

3.2.1. La Convention Européenne du 28/01/1981 pour la Protection des Personnes à l'égard du traitement informatise des données à caractère personnel.

3.2.2. La Directive de la CEE du 21/12/1988 sur l'harmonisation de la protection juridique des logiciels.

3.2.3. La Directive du Conseil des Communautés Européennes du 14 mai 1991.

3.2.4. Loi du 10 mai 1994 modifiant la loi du 1er juillet 1992 relative au Code de Propriété Intellectuelle.

3.2.5. Répression de la contrefaçon - Reproduction autre qu'une copie de sauvegarde

3 mois à 2 ans de prison et 913 à 18 266 euros d'amende.

3.2.6. Utilisation d'un logiciel non expressément autorisé

3 mois à 2 ans de prison et 913 à 18 266 euros d'amende.

Cette liste n'a rien d'exhaustif, les éléments donnés le sont à titre d'exemples.

3.3. Règles élémentaires

Quelques recommandations élémentaires, mises en oeuvre au niveau de chaque utilisateur permettent une parade de premier niveau.

Règle 1 : Tout compte utilisateur doit être doté d'un mot de passe.

Règle 2 : Changer de mot de passe régulièrement.

Règle 3 : Ne pas afficher de mot de passe, même si le poste de travail est partagé par plusieurs personnes travaillant dans le même bureau.

Règle 4 : Ne prêter jamais votre compte.

Règle 5 : Ne donner jamais votre mot de passe à un tiers.

Règle 6 : Ne pas laisser traîner de supports magnétiques (disquettes, bandes, etc...) dans un bureau ouvert.

Règle 7 : Protéger vos fichiers.

Règle 8 : Terminer proprement vos sessions, en cas d'incident ou de fin anormale, prévenir immédiatement le responsable du matériel et votre hiérarchie.

Règle 9 : Après une présentation de votre application, prenez soin de changer votre mot de passe.

Règle 10 : Ne quittez jamais votre poste de travail en laissant une session en cours.

4. DÉCLARATION DE L'UTILISATEUR

Article 1er : à qui s'applique la Charte

Tout utilisateur, étudiant, enseignant, chercheur, personnel administratif ou technique est soumis à la Charte du Bon Usage de l'informatique et des réseaux à l'Université de Provence.

Article 2 : Utilisation exclusive

Tout utilisateur s'engage à utiliser les moyens informatiques et réseaux mis à sa disposition dans le cadre exclusif de son activité à l'Université de Provence.

Article 3 : Propriété du binôme mot de passe/espace de travail

Tout utilisateur s'engage à ne pas communiquer son mot de passe et à ne pas prêter son compte à un tiers même temporairement.

Article 4 : Responsabilité de l'utilisateur

Tout utilisateur est responsable de la pérennité de ses fichiers et de l'intégrité de son espace travail et de l'utilisation qu'il fait des ressources informatiques de l'Université.

Article 5 : Engagement de non-duplication et de non-utilisation de logiciel non autorisé

Tout utilisateur s'engage à ne procéder à d'autre copie de logiciels que celles permettant la sauvegarde de ses propres données, et à ne pas utiliser de logiciel non expressément autorisé.

Article 6 : Engagement de vigilance

Tout utilisateur s'engage à signaler toute tentative de violation de son compte dès qu'il en aura connaissance. La non observation de cet article entraînant ipso facto pour l'utilisateur la fermeture immédiate de son compte et engage sa responsabilité pleine conformément à la loi article 462-8.

Article 7 : Responsabilité de la DSII

La DSII s'engage à mettre en oeuvre les sécurités réseaux dont il a connaissance, et à assurer une sauvegarde des fichiers qui sont sur la machine dont il a l'administration.

Article 8 : Sanctions

Tout contrevenant se verra sanctionner au niveau universitaire, conformément aux sanctions prévues par le règlement intérieur de l'établissement, le Président de l'Université de Provence pourra, si nécessaire, engager les poursuites au niveau pénal.

Article 9 : Durée de vie de l'habilitation à utiliser un compte

Tout utilisateur, lors de la cessation même provisoire de son activité, perd son habilitation à utiliser les moyens et ressources informatiques et réseaux de l'Université de Provence.

Article 10 : Engagement personnel

Je soussigné,..... utilisateur des Moyens Informatiques et Réseaux de l'Université en qualité d'étudiant(e) déclare avoir pris connaissance de la Charte du Bon Usage de l'informatique et des réseaux à l'Université de Provence.

Lu et approuvé, le ___/___/____

Signature