CHARTE INFORMATIQUE DE L'UNIVERSITE NANCY 2

(approuvée par le Conseil d'administration du 10 Juillet 2001)

La présente charte a pour objet de définir les règles d'utilisation des moyens informatiques au sein de l'Université Nancy 2, en particulier de préciser les responsabilités des utilisateurs, ce conformément à la législation et afin de permettre un usage normal et optimal des ressources informatiques et des services Internet employés dans l'Etablissement.

1. Champ d'application de la charte

Les règles et obligations ci-dessous énoncées s'appliquent à toute personne ; en particulier enseignants, chercheurs, enseignants-chercheurs, étudiants, personnels administratifs ou technique ; autorisée à utiliser les moyens et systèmes informatiques de l'Université de Nancy 2.
Ces derniers comprennent notamment les serveurs, stations de travail et micro-ordinateurs des services administratifs, des salles de cours ou d'informatique, des laboratoires et des Centres de Documentation de l'Université.
Le respect des règles définies par la présente charte s'étend également à l'utilisation des systèmes informatiques d'organismes extérieurs à l'Université, systèmes accessibles par l'intermédiaire des réseaux de l'établissement, par exemple le réseau Internet.

2. Conditions d'accès aux réseaux informatiques de l'Université

L'utilisation des moyens informatiques de l'Université a pour objet exclusif de mener des activités de recherche, d'enseignement ou d'administration. Sauf autorisation préalable délivrée par l'Université, ces moyens ne peuvent être employés en vue d'une utilisation ou de la réalisation de projets ne relevant pas des missions de l'Université ou des missions confiées aux utilisateurs.
Chaque utilisateur se voit attribuer des codes d'accès en fonction de ses besoins (accès internet, accès aux applications de gestion, accès à des serveurs particuliers, etc.). Les codes d'accès attribués sont strictement personnels et incessibles. Chaque utilisateur est responsable de l'utilisation qui en est faite. Le mot de passe choisi ne doit correspondre ni à un mot, ni à un nom propre d'aucune langue que ce soit. Chaque utilisateur s'engage à ne pas communiquer ce mot de passe à une tierce personne.
L'utilisateur préviendra le responsable informatique si un code d'accès ne lui permet plus de se connecter, s'il soupçonne que son compte a été usurpé. D'une façon plus générale, il informera le responsable informatique de toute anomalie qu'il pourrait constater.

3. Respect des règles de la déontologie Informatique

Chaque utilisateur s'engage à respecter les règles de la déontologie informatique et notamment à ne pas effectuer intentionnellement des opérations qui pourraient avoir pour conséquences :

- de masquer sa véritable identité ;
- de s'approprier le mot de passe d'un autre utilisateur ;
- d'altérer, de modifier des données ou d'accéder à des informations appartenant à d'autres utilisateurs du réseau ou à l'Université, sans leur autorisation ;
- de porter atteinte à l'intégrité d'un autre utilisateur ou à sa sensibilité, notamment par l'intermédiaire de messages, textes ou images provocants ;
- d'interrompre ou de perturber le fonctionnement normal du réseau ou d'un des systèmes connectés au réseau ; · de modifier ou de
- détruire des informations sur un des systèmes ;
- de se connecter ou d'essayer de se connecter sur un site sans y être autorisé.

La réalisation d'un programme informatique ayant de tels objectifs est également interdite.
Si dans l'accomplissement de son travail ou de ses missions, l'utilisateur est amené à constituer des fichiers, il est rappelé que la loi " informatique et libertés" impose, préalablement à leur constitution,

que les fichiers comportant un traitement de données nominatives fassent l'objet d'une déclaration ou d'une demande d'avis auprès de la Commission Nationale Informatique et Libertés (CNIL). Pour plus d'informations, contact : Service des Affaires Générales de l'Université

4. Utilisation de logiciels

L'utilisateur ne peut installer un logiciel qu'après avis du service informatique compétent.
L'utilisateur ne devra en aucun cas :

- installer des logiciels à caractère ludique ;
- faire une copie d'un logiciel commercial ;
- contourner les restrictions d'utilisation d'un logiciel ;
- développer des programmes constituant ou s'apparentant à des virus.

5. Utilisation des moyens informatiques

Chaque utilisateur s'engage à prendre soin du matériel et des locaux informatiques mis à sa disposition. Il informe le service informatique de toute anomalie constatée. L'utilisateur doit s'efforcer de n'occuper que la quantité d'espace disque qui lui est strictement nécessaire et d'utiliser de façon optimale les moyens de compression des fichiers dont il dispose. L'utilisation des ressources doit être rationnelle et loyale afin d'en éviter la saturation.
Tout ordinateur propre à un département, laboratoire ou service, doit être connecté au réseau par l'intermédiaire d'un informaticien de l'Université. Ce dernier s'assure en particulier que les règles de sécurité sont bien respectées.

Un utilisateur ne doit jamais quitter un poste de travail en libre service sans se déconnecter.

6. Dispositions particulières pour les utilisateurs étudiants

Gestion des boîtes aux lettres des étudiants
Tous les étudiants de Nancy 2 disposent d'une boîte aux lettres personnelle. La taille de celle-ci est limitée. Pour éviter des dysfonctionnements du service de messagerie, le Centre de Ressources Informatiques pourra être amené à supprimer les messages les plus anciens dans le cas où les boîtes aux lettres ont atteint une taille maximale. D'une façon plus générale, des modifications des paramètres de messagerie pourront être faites pour assurer le fonctionnement.

7. Information des utilisateurs sur la gestion des systèmes et réseaux informatiques

Responsabilités des administrateurs systèmes/réseau/SGBD
Les administrateurs systèmes/réseau/SGBD sont les personnes qui gèrent les machines connectées au réseau de l'Université ainsi que les serveurs sur lesquels sont installés les différents services mis à la disposition des utilisateurs (services Internet, applications de gestion, services pédagogiques, services pour la recherche et la documentation).

- Les administrateurs ont la charge de la bonne qualité du service fourni aux utilisateurs dans la limite des moyens alloués. Ils ont le droit d'entreprendre toute démarche nécessaire au bon fonctionnement des moyens informatiques de l'Université;
- Les administrateurs ont le devoir d'informer, dans la mesure du possible, les utilisateurs de toute intervention nécessaire, susceptible de perturber ou d'interrompre l'utilisation habituelle des moyens informatiques;
- Les administrateurs ont le devoir d'informer immédiatement le responsable sécurité de l'université (ou son suppléant) de toute tentative d'intrusion sur un système, ou de tout comportement délictueux d'un utilisateur;
- Les administrateurs doivent impérativement respecter la confidentialité des fichiers des utilisateurs.

Fichiers de traces
L'ensemble des services utilisés génèrent, à l'occasion de leur emploi, "des fichiers de traces". Ces fichiers sont essentiels à l'administration des systèmes. Ils servent en effet à remédier aux dysfonctionnements des services ou systèmes informatiques utilisés. Ces fichiers conservent des informations par exemple concernant la messagerie (expéditeur, destinataire(s), date), mais aussi heures de connexion aux applications de gestion, au service de connexion à distance, numéro de la machine depuis laquelle les services sont utilisés, etc.
Ce type de traces existent pour l'ensemble des services Internet. Ces fichiers ne sont utilisés que pour un usage technique. Toutefois, dans le cadre d'une procédure judiciaire et après accord du Président ces fichiers peuvent être mis à la disposition ou transmis à la justice.

Les virus
Des outils sont également mis en place pour protéger les postes des utilisateurs contre les virus.

- Les logiciels anti virus sur les postes des utilisateurs sont paramétrés avec la stratégie suivante: Si un virus est détecté, le logiciel tente de réparer le fichier, si la tentative échoue, le fichier est détruit.
- Un logiciel d'anti virus est également mis en place sur les serveurs de messagerie évitant ainsi de recevoir des virus et aussi d'en émettre à l'extérieur de Nancy 2. Le destinataire et l'expéditeur sont informés que le message contenait un virus et le message n'est pas délivré.
- D'autres logiciels pourront être mis en place pour protéger au mieux les données des utilisateurs et les applications de l'Université.

L'utilisateur qui contreviendrait aux règles précédemment définies s'expose au retrait de son compte informatique, ainsi qu'aux poursuites disciplinaires et pénales, prévues par les textes législatifs et réglementaires en vigueur.

Pour mémoire, les autres textes de référence en matière informatique sont :
- la loi « informatique et libertés » de Janvier 1978 (création de la CNIL),
- la loi de Juillet 1978 sur l'accès aux documents administratifs,
- la loi de 1985 sur la protection des logiciels,
- la loi du 5 janvier 1988 relative à la fraude informatique,
- les règles de bonne conduite pour l'utilisateur du réseau StanNet.
- la charte Renater

LOI n° 88-19 du 5 Janvier 1988 relative à la fraude informatique

L'Assemblée Nationale et le Sénat ont adopté,
Le Président de la République promulgue la loi dont la teneur suit :

Article unique - Dans le titre II du livre III du code pénal, il est inséré, après le chapitre II, un chapitre III ainsi rédigé :

Chapitre III
De certaines infractions en matière informatique

Article 462-2 - Quiconque, frauduleusement, aura accédé ou se sera maintenu dans tout ou partie d'un système de traitement automatisé de données sera puni d'un emprisonnement de deux mois à un an et d'une amende de 304.90 € à 7622.45 €. ou de l'une de ces deux peines. Lorsqu'il en sera résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, l'emprisonnement sera de deux mois à deux ans et l'amende de 1524.49 €. à 15244.90 €.

Article 462-3 - Quiconque aura, intentionnellement et au mépris des droits d'autrui, entravé ou faussé le fonctionnement d'un système de traitement automatisé de données sera puni d'un emprisonnement de trois mois à trois ans et d'une amende de 1524.49 €. à 15244.90 € ou de l'une de ces deux peines.

Article 462-4 - Quiconque aura, intentionnellement et au mépris des droits d'autrui, directement ou indirectement, introduit des données dans un système de traitement automatique ou supprimé ou modifié les données qu'il contient ou leurs modes de traitement ou de transmission, sera puni d'un emprisonnement de trois mois à trois ans et d'une amende de 304.90 €. à 76224.51 €. ou de l'une de ces deux peines.

Article 462-5 - Quiconque aura procédé à la falsification de documents informatisés, quelle que soit leur forme, de nature à causer un préjudice à autrui, sera puni d'un emprisonnement d'un an à cinq ans et d'une amende de 3048.98 €. à 30489.80 €.

Article 462-6 - Quiconque aura sciemment fait usage des documents informatisés visés à l'article 462-5 sera puni d'un emprisonnement d'un an à cinq ans et d'une amende de 3048.98 € à 30489.80 €. ou de l'une de ces deux peines.

Article 462-7 - La tentative des délits prévus par les articles 462-2 à 462-6 est punie des mêmes peines que le délit lui-même.

Article 462-8 - Quiconque aura participé à une association formée ou à une entente établie en vue de la préparation, concrétisée par un ou plusieurs faits matériels, d'une ou de plusieurs infractions prévues par les articles 462-2 à 462-6 sera puni des peines prévues pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée.

Article 462-9 - Le tribunal pourra prononcer la confiscation des matériels appartenant au condamné et ayant servi à commettre les infractions prévues au présent chapitre.
