Charte de l'Université des Sciences et Technologies de Lille pour le bon usage de l'informatique et des réseaux

La présente charte a pour objet de définir les quelques règles simples mais importantes d'utilisation 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'Université des Sciences et Technologies de Lille comprennent notamment les serveurs, stations de travail et micro-ordinateurs des services administratifs et techniques, des laboratoires, des salles communes de cours, etc.
Ces termes englobent également tout logiciel ou matériel affecté au fonctionnement du réseau d'établissement.

1. Domaine d'application

Les règles et obligations définies dans cette charte s'appliquent à tout utilisateur des moyens informatiques de l'établissement ainsi que des moyens informatiques extérieurs accessibles via les réseaux informatiques de l'Université des Sciences et Technologies de Lille.
On appelle “Utilisateur” toute personne, quelque soit son statut : étudiant, enseignant, chercheur, ingénieur, technicien, administratif, personnel temporaire, stagiaire, ... appelée à utiliser les ressources informatiques et réseau de l'établissement.

2. Conditions d'accès

Le droit d'accès d'un utilisateur à un système informatique est soumis à autorisation. Il est personnel et incessible, et disparaît lorsque les raisons de cet accès disparaissent. Ce droit est limité à des activités conformes aux missions de l'établissement (recherche, enseignement, administration).
Chaque utilisateur est tenu pour responsable de toute utilisation des ressources informatiques auxquelles il a accès. Lorsque l'utilisation d'un système informatique implique l'ouverture d'un compte nominatif, l'utilisateur ne doit pas se servir, pour y accéder, d'un autre compte que celui qui lui a été attribué par l'administrateur habilité. Sauf autorisation écrite du chef d'établissement ou du responsable de service, les moyens informatiques ne peuvent être utilisés pour d'autres activités, notamment commerciales "hors mission de l'université"
La connexion d'un système informatique au réseau est soumise à accord du service responsable, après signature de cette charte par le responsable du système.
Tout utilisateur devra respecter les modalités de raccordement des matériels au réseau de l'établissement. Ces modalités sont établies par les responsables informatiques.
Tout ordinateur propre à un département, laboratoire ou service, devant être connecté au réseau devra être déclaré au service responsable de la gestion du réseau (CRI), et devra être géré par un administrateur qui est responsable de son bon fonctionnement. Ce dernier doit en particulier s'assurer que les règles de sécurité et de confidentialité sont bien respectées.

3. Confidentialité (Respect de la / Conditions de)

Les fichiers possédés par des utilisateurs doivent être considérés comme privés qu'ils soient ou non accessibles à d'autres utilisateurs. Le droit de lecture ou de modification d'un fichier ne peut être réalisé qu'après accord explicite de son propriétaire.
En particulier, il est interdit de prendre connaissance d'informations détenues par d'autres utilisateurs, quand bien même ceux-ci ne les auraient pas explicitement protégées. Cette règle s'applique également aux conversations privées de type messagerie électronique dont l'utilisateur n'est destinataire ni directement, ni en copie.
Les utilisateurs sont tenus à la réserve d'usage sur toute information relative au fonctionnement interne de l'établissement qu'ils auraient pu obtenir en utilisant les ressources informatiques.
Les administrateurs de systèmes peuvent être amenés (avec l'autorisation du responsable de service, de laboratoire, ou d'UFR) à examiner le contenu de fichiers, boîte aux lettres, de façon à obtenir suffisamment d'informations pour corriger des problèmes logiciels 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.
Si, dans l'accomplissement de son travail, l'utilisateur est amené à constituer des fichiers tombant sous le coup de la loi Informatique et Libertés, il devra auparavant en avoir fait la demande à la CNIL et en avoir reçu l'autorisation. On rappelle que cette autorisation n'est valable que pour le traitement défini dans la demande et pas pour le fichier lui-même.
Les postes de travail individuels ne doivent pas être utilisés sans la permission des personnes à qui ils sont attribués.

4. Respect des droits de propriétés

Il est interdit à tout utilisateur de faire des copies de logiciels commerciaux pour quelque usage que ce soit. Les copies de sauvegardes 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. Informatique et liberté

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).
Selon la loi, une information nominative est une information qui permet l'identification, sous quelque forme que ce soit d'une personne physique (exemple : adresse électronique).
Toute personne enregistrée dans une base doit être informée de la forme des données et de l'utilisation qui en est faite.
De plus, elle doit avoir la possibilité d'y avoir accès et de faire rectifier toute information erronée la concernant.

6. Les principes à 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 normal 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 normal du réseau ou des systèmes connectés au réseau (manipulations anormales, introduction de VIRUS, ...);
- de se connecter ou d'essayer de se connecter sur un site extérieur à l'établissement sans y être autorisé;
- d'accéder au compte d'un autre utilisateur sans l'autorisation de celui-ci
- 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, en particulier des informations comptables ou d'identification;
- de porter atteinte à l'intégrité d'un autre utilisateur ou à sa sensibilité, notamment par l'intermédiaire de messages, textes ou images provoquants;
- de masquer sa véritable identité, en particulier en se connectant sous le nom d'un autre utilisateur,
- de développer des outils mettant sciemment en cause l'intégrité des systèmes;
- de nuire à l'image de marque de l'établissement par une mauvaise utilisation des outils réseaux.

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 de recommandations fournies par les administrateurs et les responsables de l'outil informatique.

Parmi les règles de bon usage (de bon sens) :

- user raisonnablement de toutes les ressources partagées (puissance de calcul, espace disque, logiciels à jetons, bande passante sur le réseau, ...);
- ne jamais quitter son poste de travail en laissant une session ouverte;
- ne pas laisser un document affiché sur l'écran de visualisation après exploitation;
- protéger ses fichiers, avec l'aide éventuelle des administrateurs; l'utilisateur est responsable des droits qu'il accorde à des tiers;
- choisir des mots de passe sûrs respectant les recommandations des administrateurs. Ces mots de passe doivent être tenus secrets
  * ne pas les écrire sur un document papier,
  * ne jamais les communiquer à un tiers
  * les changer régulièrement;
- ne jamais prêter son compte;
- sauvegarder régulièrement ses fichiers;
- contrôler l'accès des locaux où sont situés des équipements informatiques;

7. Sanctions applicables

Des lois et textes réglementaires définissent les droits et obligations des personnes utilisant les moyens informatiques.

Tout utilisateur n'ayant pas respecté les lois peut être poursuivi pénalement. De plus les utilisateurs ne suivant pas les règles et obligations définies dans cette charte sont passibles de sanctions internes à l'établissement, dans le cadre de l'application des textes du règlement intérieur. Le non-respect des règles déontologiques se traduit 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 des Sciences et Technologies de Lille, avec l'accord de son Conseil d'Administration est habilité à saisir le Procureur de la République.

8. Responsabilité et devoir de l'établissement

L'établissement, 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'établissement 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. L'établissement ne fournit aucune garantie, implicite ou explicite, quant à l'exactitude des résultats obtenus par l'utilisation de ses moyens informatiques.

RAPPEL DE QUELQUES TEXTES DE LOI

Protection des personnes : Loi du 6 janvier 1978 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. (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 Les 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 secrets des correspondances (écrites, transmises par voie de télécommunications) Accès ou maintien frauduleux dans un système informatique
La 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 (max dans le cas de modification du système)
Art 323-5 peines complémentaires