Charte de l'université de Cergy-Pontoise
pour le bon usage de l'informatique et des réseaux

La présente charte définit les règles d'utilisation des moyens informatiques de l'université de Cergy-Pontoise (UCP).

■ Domaine d'application

a) Définition des ressources informatiques

Ce document utilise indifféremment les termes moyens, systèmes ou ressources informatiques. Ces termes englobent l'ensemble des matériels, logiciels et bases de données ayant trait aussi bien aux ordinateurs qu'au réseau d'établissement. Les moyens informatiques de l'UCP comprennent notamment les ordinateurs, serveurs, stations de travail et micro-ordinateurs des services administratifs et techniques, des laboratoires, des centres de documentation, des salles d'enseignement, etc. Sont également inclus tous les équipements de réseaux tels que ponts, commutateurs, routeurs, modems, multiplexeurs, etc.

b) Utilisateurs

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

■ Conditions d'accès et raccordement

a) Accès

Le droit d'accès d'un utilisateur à un système informatique est soumis à autorisation. Il ne peut être utilisé que dans le cadre de l'activité professionnelle des utilisateurs conformément à la législation en vigueur. Il est personnel et incessible. Ce droit prend fin lors de la cessation, même temporaire, des activités ayant permis à l'utilisateur de disposer des ressources informatiques. Ce droit est limité à des activités conformes à la fois

– à la charte d'usage et de sécurité de RENATER (disponible à http://www.cru.fr/droit-deonto/deontologie/chartes/renater-v12.ps).
– aux missions de l'université (recherche, enseignement, administration)

Sauf autorisation écrite du chef d'établissement, les moyens informatiques ne peuvent être utilisés pour d'autres activités, notamment commerciales.

Chaque utilisateur est tenu pour responsable de toute utilisation des ressources informatiques faite à partir de son poste ou de son compte. L'utilisation du poste de travail personnel ou des fichiers d'un tiers exige l'accord formel de ce dernier.

b) Raccordement

La connexion, ainsi que tout changement de raccordement, d'un système informatique au réseau sont soumis à l'accord du service réseaux & sécurité. Toute machine connectée est placée sous la responsabilité d'une personne qui doit obligatoirement être déclarée au service réseaux & sécurité : pour les postes individuels (type PC, Mac ou stations), le responsable par défaut est l'attributaire du poste ; pour les ordinateurs assurant des services réseaux ou les machines à usage collectif, deux responsables seront désignés, un titulaire et un suppléant, ayant les droits administrateur. Au préalable, la signature de la présente charte par le(s) responsable(s) du système est obligatoire.

Les matériels et logiciels doivent être conformes aux normes. Le demandeur est tenu de fournir toutes informations utiles quant aux interfaces, protocoles, logiciels et matériels interagissant d'une manière ou l'autre avec le réseau. Il devra vérifier que la machine à brancher satisfait toutes les conditions de sûreté et de fiabilité, et que son usage ne nuira pas au bon fonctionnement du réseau.

Il importe aussi que, dès le début, la liste ou la catégorie de personnes à qui est destiné l'usage de la machine soit clairement définie et conforme à la sectorisation des réseaux. Le responsable s'engage à respecter et à mettre en œuvre tous les moyens nécessaires pour que soit respectée la classe d'accès. Tout changement de la classe d'accès (par extension, restriction ou changement d'affectation) doit faire l'objet d'un accord avec les services réseaux.

Le responsable se conformera aux règles d'usage du réseau pour l'installation et l'exploitation de sa machine. Il optera pour des systèmes d'exploitation sécurisés, garantissant une bonne authentification de l'identité des utilisateurs. Veiller à ce que l'accès à la machine soit contrôlé, soit au niveau de la machine (mots de passe) soit au niveau du local (verrous).

En dehors du service réseaux & sécurité, il est interdit de connecter une machine à la fois sur le réseau informatique d'établissement et sur un autre réseau (par ex. téléphonique). De même, sauf dérogation visée par le chef du service réseaux, il est interdit de connecter une même machine sur plusieurs sous-réseaux à la fois. Dans tous les cas, ceux qui réalisent ou commandent ce genre d'interconnexion seront tenus pour responsables de toute intrusion passant par ce canal.

En cas d'urgence et de danger flagrant, le service réseaux & sécurité est autorisé à déconnecter une prise.

■ Confidentialité

Les fichiers possédés par des utilisateurs doivent être considérés comme privés même s'ils sont accessibles à d'autres utilisateurs. 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 e-mail 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.

Pour des nécessités de maintenance et de gestion techniques, l'utilisation des ressources matérielles ou logicielles ainsi que les échanges via le réseau peuvent être analysés et contrôlés dans le respect de la législation applicable et, notamment, de la loi sur l'informatique et les libertés.

Les administrateurs de systèmes pourront donc être amenés à examiner le contenu des fichiers, boîtes aux lettres, ou autres ressources informatiques, uniquement afin de corriger les problèmes de fonctionnement ou, s'il y a lieu, de déterminer si un utilisateur ne respecte pas la politique d'utilisation des ressources informatiques de l'établissement.

Cet examen des contenus se fera sur autorisation de l'utilisateur ou, en cas d'absence, de congés ou de tout événement rendant impossible l'expression personnelle de l'utilisateur, avec l'autorisation de son responsable (supérieur hiérarchique, responsable de service, de laboratoire, d'UFR ou tout autre responsable d'entité autonome).

Les administrateurs de systèmes préserveront la confidentialité des informations privées qu'ils seront amenés à connaître dans ce cadre.

■ Respect des droits de propriété

Il est interdit de faire des copies de logiciels commerciaux en dehors des clauses spécifiées par les contrats. 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 interdit d'utiliser un logiciel sur un système sans s'être assuré préalablement que les droits de licence le permettent.

Néanmoins, les fournisseurs ou leurs relais internes veilleront à ménager une période de test suffisante mais strictement limitée (en général de l'ordre d'un mois) pour permettre à l'acheteur de vérifier fiabilité et compatibilité du logiciel avec le support matériel.

■ 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 en être informée. Elle a droit de regard sur la forme des données et l'utilisation qui en est faite. De plus, elle doit pouvoir avoir accès à toute information la concernant et y faire rectifier toute erreur. L'usager et le personnel reçoit une adresse électronique de l'université de Cergy-Pontoise. En signant cette charte, il accepte la création de cette adresse et de recevoir les messages émis par l'université, afférents à la vie de l'établissement et universitaire notamment via les lettres électroniques créées dans ce but, afin de faciliter l'information des étudiants et personnels et l'organisation de la vie universitaire.

■ Sécurité

a) Tout utilisateur est responsable de l'utilisation qu'il fait des ressources informatiques ; il s'engage à n'effectuer aucune opération qui pourrait nuire au fonctionnement normal du réseau, à l'intégrité des moyens informatiques, ou aux relations internes et externes de l'établissement. 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 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 sans leur autorisation ;
– de modifier ou détruire des informations appartenant à des tiers 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 mensongers ou diffamatoires ;
– de masquer sa véritable identité, en particulier en se connectant sous le nom d'un autre utilisateur ;
– de développer ou d'utiliser des outils mettant sciemment en cause l'intégrité des systèmes ;
– de nuire à l'établissement par une mauvaise utilisation des outils réseaux.

b) La sécurité est l'affaire de tous.

Chaque utilisateur doit y contribuer à son niveau, et mettre en application les règles de bon sens et les recommandations fournies par les administrateurs et responsables informatiques. Parmi les règles de bon sens et de bon usage :

– user raisonnablement de toutes les ressources partagées (puissance de calcul, espace disque, logiciels à jetons, bande passante sur le réseau…) ;
– ne jamais quitter un poste de travail en laissant une session ouverte ;
– ne laisser aucun 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 ;
– suivre les recommandations des administrateurs en matière de mots de passe. Ces mots de passe doivent être choisis non transparents et tenus secrets. Il faut donc ne jamais les écrire sur un support matériel ni les communiquer à un tiers. Il convient de les changer régulièrement ;
– ne jamais prêter son compte sans contrôle ;
– ne pas utiliser ou essayer d'utiliser des comptes autres que le sien ou masquer sa véritable identité ;
– sauvegarder régulièrement ses fichiers ;
– contrôler l'accès des locaux où sont situés les équipements ;
– signaler aux administrateurs toute violation, tentative de violation ou violation suspectée d'un système informatique. De même, leur signaler toute faille de protection, anomalie de fonctionnement, etc. portant atteinte au bon niveau de sécurité ;
– respecter les consignes des administrateurs systèmes et des responsables informaticiens.

■ Sanctions applicables

Des lois et règlements définissent les droits et obligations des personnes utilisant les moyens informatiques. Tout utilisateur n'ayant pas respecté ces textes 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, en application des statuts. Les cas de fraude, de non respect des règles, les atteintes au bon fonctionnement de l'établissement sont soumis à la commission disciplinaire de l'UCP qui prononce les sanctions. Le Président de l'université peut déclencher des poursuites et obtenir réparation devant les tribunaux judiciaires.

■ Responsabilité et devoirs de l'établissement

L'établissement est lui-même soumis aux règles de bon usage 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 aux règles énoncées dans cette charte. L'établissement ne fournit aucune garantie, implicite ou explicite, quant à l'exactitude des résultats obtenus par l'utilisation de ses moyens informatiques

■ Rappel des lois les plus importantes

Accès ou maintien frauduleux dans un système informatique

– Art. 323-1 à 323-7 du Code Pénal relatifs à la fraude informatique.
– Loi 92-684 du 22 juillet 1992 (déclaration préalable à la création de tout fichier contenant des informations nominatives).
– Art. 226-16 à 226-23 du Code Pénal: atteintes au droit de la personne résultant des fichiers ou des traitements informatiques;
– Art. 226-24 du Code Pénal instituant la responsabilité pénale des personnes morales pour ces mêmes infractions (art. 226-16 à23).
– Convention Européenne du 28/01/1981.

Protection des logiciels

– Lois du 3 juillet 1985 et du 1er juillet 1992 sur la protection des logiciels. Protection des droits d'auteur, et interdiction 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 1erjuillet 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

Loi n°91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des télécommunications

– Art. 432-9 et 226-15 al.1 du Code Pénal secrets des correspondances (écrites, transmises par voie de télécommunications).
– Art. 413-9 et suivants du code pénal relatifs aux atteintes au secret de la défense nationale et 411-6 et suivants concernant la livraison d'informations à une puissance étrangère.
– Art. 414-5 peines complémentaires.

Réglementation des télécommunications

Loi n°90-1170 du 29 décembre 1990 relative à la réglementation des télécommunications.

Certains de ces textes sont disponibles à la Bibliothèque universitaire (Code Pénal) et sous ftp://ftp.

Je soussigné(e) .....

Service/dép./filière .....

UFR .....

utilisateur des moyens informatiques et réseaux de l'UCP, déclare avoir pris connaissance de la présente charte de bon usage de l'informatique et des réseaux et m'engage à la respecter.

Signature précédée de la mention "lu et approuvé"

Date .....