

CHARTRE DE BON USAGE DE L'INFORMATIQUE ET DES RÉSEAUX À L'UNIVERSITÉ ROBERT SCHUMAN

Les équipements informatiques de l'Université Robert Schuman et des autres institutions partenaires à la gestion du réseau Osiris sont dédiés à l'enseignement, la recherche et l'administration. La plupart de ces équipements sont reliés au réseau Osiris, et par cet intermédiaire, au réseau Internet. Tout utilisateur de ces équipements appartient donc à une vaste communauté, ce qui implique de sa part le respect de certaines règles de sécurité et de bonne conduite, l'imprudence, la négligence ou la malveillance d'un utilisateur pouvant avoir des conséquences graves pour la communauté. La présente charte définit les droits et les devoirs de chacun et représente un engagement mutuel entre l'utilisateur et la communauté universitaire.

Les différents acteurs

Du point de vue informatique, il faut distinguer trois catégories d'acteurs dans la communauté universitaire :

- les utilisateurs : étudiants, enseignants, chercheurs, personnels utilisant les systèmes informatiques mis à leur disposition,
- les administrateurs systèmes et/ou réseau, responsables techniquement du bon fonctionnement des outils informatiques,
- les responsables fonctionnels : les Directeurs d'U.F.R., les Responsables Administratifs, les Directeurs de laboratoire ou de service, les enseignants encadrant des étudiants dans le cadre d'activités faisant appel à des ressources informatiques.

Chacun a des droits et des devoirs identiques dans l'esprit mais différents dans la pratique.

Les droits de tous

Chacun a droit à :

- l'information relative aux ressources et aux services communs offerts par l'Université, l'U.F.R., l'Ecole, l'Institut ou le Centre de Recherche,
- l'information lui permettant d'utiliser au mieux les moyens mis à sa disposition,
- l'information sur la sécurité du système qu'il utilise.

Les devoirs de chacun

- Chacun a le devoir de respecter les règles de sécurité applicables au système qu'il utilise ; ces règles consistent en la présente charte illustrée par des annexes régulièrement actualisées, ainsi qu'éventuellement les règles spécifiques liées à un environnement de travail particulier (laboratoire, salle de ressources pour étudiants) ; ces règles sont tenues à la disposition de chaque utilisateur par le responsable fonctionnel ou l'administrateur système.
- Chacun doit respecter la propriété intellectuelle et commerciale conformément à la législation en vigueur.

- Chacun s'engage à ne pas prendre connaissance d'informations appartenant à autrui sans son accord, à ne pas communiquer à un tiers de telles informations, ou des informations non publiques auxquelles il peut accéder, mais dont il n'est pas propriétaire.
- Chacun doit s'identifier clairement, nul n'a le droit d'usurper l'identité d'autrui ou d'agir de façon anonyme. Nul ne peut céder ses droits à autrui.
- Chacun doit s'efforcer de parvenir à son but par le moyen le moins "coûteux" en ressources communes (espace disque, impressions, occupation des postes de travail, transferts réseau, occupation de serveurs distants, ...).
- Chacun doit contribuer à l'amélioration du fonctionnement et de la sécurité des outils informatiques, en respectant les règles et conseils de sécurité, en signalant immédiatement aux responsables toute anomalie constatée, en sensibilisant ses collègues aux problèmes dont il a connaissance.
- Chacun doit se limiter à un usage professionnel des équipements mis à sa disposition et respecter la fonction qui leur est assignée, ce qui exclut l'utilisation à des fins personnelles, l'utilisation dans un but commercial, l'utilisation abusive d'un équipement de l'enseignement pour la recherche et vice-versa. Nul ne peut modifier un équipement, tant du point de vue matériel que logiciel système, sans l'accord du responsable du système.

Droits et devoirs spécifiques des administrateurs système et/ou du réseau

Sur les nombreux systèmes, l'administrateur a techniquement tous les pouvoirs, il a de ce fait des devoirs importants, en particulier celui de ne pas abuser de ses pouvoirs. D'après le code pénal, l'administrateur système est personnellement responsable de la sécurité de la machine et/ou du réseau dont il a la charge.

Tout administrateur système a le droit :

- d'être informé des implications légales de son travail, en particulier des risques qu'il court dans le cas où un utilisateur du système dont il a la charge commet une action répréhensible,
- d'accéder aux informations privées à des fins de diagnostic et d'administration du système, en respectant scrupuleusement la confidentialité de ces informations,
- d'établir des procédures de surveillance des actions de non-respect de la présente charte, après autorisation de son responsable fonctionnel et en relation avec le correspondant sécurité du réseau...

Tout administrateur système a le devoir :

- d'informer les utilisateurs sur l'étendue des pouvoirs dont lui-même dispose techniquement de par sa fonction,
- d'informer les utilisateurs et de les sensibiliser aux problèmes de sécurité informatique inhérents au système, de leur faire connaître les règles de sécurité à respecter, aidé par le correspondant sécurité du réseau,
- de respecter les règles générales d'accès au réseau définies pour le réseau Osiris,
- de respecter les règles de confidentialité, en limitant au strict nécessaire l'accès à l'information confidentielle et en respectant un "secret professionnel" sur ce point,
- de respecter, s'il est lui-même utilisateur du système, les règles qu'il est amené à imposer aux autres utilisateurs,
- de modifier le système dans le sens d'une meilleure sécurité, dans l'intérêt des utilisateurs,
- d'informer immédiatement son responsable fonctionnel et le correspondant sécurité de l'Université de toute tentative (fructueuse ou non) d'intrusion sur son système, ou de tout comportement dangereux d'un utilisateur,
- de coopérer avec les correspondants sécurité du réseau en cas d'attaque impliquant une machine qu'il administre.



Droits et devoirs spécifiques des responsables fonctionnels

Les responsables fonctionnels de systèmes informatiques ont le droit :

- d'interdire l'accès des outils informatiques à un utilisateur qui ne respecte pas la présente charte,
- de saisir l'autorité hiérarchique des manquements graves résultant du non respect de cette charte, le Président de l'Université Robert Schuman pouvant déclencher des procédures disciplinaires ou pénales.

Les responsables fonctionnels de systèmes informatiques ont le devoir :

- d'informer tous les acteurs, de diffuser la présente charte par tous moyens appropriés,
- de communiquer au correspondant sécurité du réseau le nom des responsables système de toutes les machines placées sous leur autorité et au Centre Réseau Communication le nom d'un responsable réseau,
- de soutenir de leur autorité les administrateurs système dans leur travail de mise en application de cette charte.

Sanctions encourues en cas de non respect

Le non respect des règles définies dans cette charte peut entraîner des sanctions de nature :

- disciplinaire :
 - ⇒ les responsables fonctionnels ont pleine autorité pour prendre les mesures conservatoires nécessaires en cas de manquement à la présente charte et interdire aux utilisateurs fautifs l'accès aux moyens informatiques et au réseau,
 - ⇒ ces utilisateurs fautifs peuvent être déférés devant l'instance disciplinaire compétente,
- pénale :

L'évolution des techniques électroniques et informatiques a conduit le législateur à définir des sanctions pénales d'une grande sévérité à la mesure du risque que peut faire courir aux libertés individuelles l'usage incontrôlé des fichiers ou des traitements informatiques.

Cette charte est portée à la connaissance de tous les utilisateurs et s'impose à tous.

Annexe I

LA LÉGISLATION APPLICABLE EN FRANCE À L'INFORMATIQUE

Protection des personnes

- La loi du 6 janvier 1978 sur l'informatique et les libertés : elle 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 : elle impose une déclaration préalable à la création de tout fichier contenant des informations nominatives
- Article 226-24 du Nouveau Code Pénal (NCP) : il institue la responsabilité des personnes morales en cas d'infractions aux dispositions de la loi sur les atteintes à la personnalité.
- Convention Européenne du 28/01/1981

Protection des logiciels

- Lois du 3 juillet 1985 et du 1er juillet 1992 sur la protection des logiciels : elles protègent les droits d'auteur. Elles interdisent en particulier à l'utilisateur d'un logiciel toute reproduction autre que celle à usage de 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 du NCP : protection des secrets économiques et industriels.
- Art. 432-9 al. et 226-15 al. 1 du NCP : protection du secret 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 : loi la plus importante et la plus astreignante, elle énumère les peines encourues par les personnes portant atteinte aux systèmes de données.
- Art. 323-1 et suivant du NCP : il prévoit une peine d'1 à 2 ans d'emprisonnement et 100 000 à 200 000 F d'amende (maximum infligé dans le cas de modification du système).
- Art. 323-5 du NCP : il prévoit des peines complémentaires.

Annexe II

ENGAGEMENT PERSONNEL

Je soussigné _____

OSIRIS utilisateur des moyens informatiques de l'Université Robert Schuman et du réseau

déclare avoir reçu et pris connaissance de la Charte de bon usage de l'informatique et des réseaux à l'Université Robert Schuman et m'engage à la respecter.

A _____, le _____

Signature précédée de la mention
"Lu et approuvé" écrite de la main
du signataire :