# Charte du bon usage des moyens informatiques et du réseau

*Texte approuvé par le Conseil d'Administration de l'Université le 3 juillet 2006*


1. Domaine d'application ..... 1
2. Sécurité ..... 1
   2.1 Accès aux ressources informatiques : ..... 1
   2.2 Droits et devoirs de l'utilisateur : ..... 2
   2.3 Droits et devoirs des administrateurs : ..... 2
   2.4 Mesures de contrôle de la sécurité ..... 3
   2.5 Sécurité du poste de travail ..... 3
3. Usages des services Internet (Web, messagerie, forum) ..... 3
4. Propriété intellectuelle ..... 3
5. Respect de la loi informatique et libertés ..... 4
6. Rappel des principales lois françaises ..... 4
7. Sanctions ..... 4



**Université Toulouse III Paul Sabatier**
**IUT de Tarbes**

La présente charte a pour objet de formaliser les règles de déontologie et de sécurité que les Utilisateurs s'engagent à respecter en contrepartie de la mise à disposition des ressources informatiques de l'Université Paul Sabatier.

# 1. Domaine d'application

Les règles et obligations énoncées ci-dessous s'appliquent à tout utilisateur des matériels, systèmes, logiciels et réseaux informatiques de l'Université Paul Sabatier. Est déclaré utilisateur toute personne qui fait usage des ressources informatiques de l'Université Paul Sabatier. L'utilisateur est responsable, en tout lieu, de l'usage qu'il fait des ressources informatiques.
L'administrateur est une personne compétente en matière informatique et de réseaux à qui a été attribuée la fonction de gestion de tout ou partie de la sécurité des systèmes d'information et/ou de télécommunication. A ce titre, il possède des droits étendus quant à la visibilité et à la gestion des moyens informatiques et de télécommunication.
Les installations de l'Université permettant de se connecter ou de dialoguer avec des sites informatiques dans le monde entier, les règles définies par la présente charte s'étendent également à l'utilisation des ressources des réseaux extérieurs, accessibles par l'intermédiaire de réseaux d'interconnexion comme RéMiP2000, RENATER et Internet.
Le non-respect des règles de bonne conduite énoncées dans le présent document engage la responsabilité personnelle de l'utilisateur.
L'établissement, par sa signature de la charte du réseau RENATER, est lui-même soumis aux règles de bonne utilisation des moyens informatiques et, à ce titre, se doit de faire respecter les règles déontologiques et la loi.

# 2. Sécurité

## 2.1 Accès aux ressources informatiques :

Le droit d'accès est limité à des activités conformes aux missions de l'établissement : la formation initiale et continue, la recherche scientifique et technologique ainsi que la valorisation de ses résultats, la diffusion de la culture et de l'information scientifique et technique, la coopération internationale (article 4 de la loi numéro 84- 52 du 26 janvier 1984), la vie universitaire et à l'activité syndicale. Par ailleurs, l'étendue des ressources informatiques auxquelles l'utilisateur a accès peut être limitée en fonction des besoins réels et des contraintes imposées par le partage de ces ressources avec les autres utilisateurs.
Le droit d'accès est temporaire, il est retiré si la qualité de l'utilisateur ne le justifie plus. Il peut également être retiré, par mesure conservatoire du Président de l'Université, si le comportement d'un utilisateur n'est plus compatible avec les règles énoncées dans la présente charte.
Les informations permettant de se connecter au système d'information (messagerie, forum, compte utilisateur, …) sont strictement personnelles. Chaque utilisateur est responsable de l'utilisation qui en est faite. Nul n'est autorisé à utiliser les informations personnelles d'autrui.
La connexion au réseau de tout ordinateur propre à un département, laboratoire ou service, doit se faire sous contrôle d'un administrateur. Ce dernier doit s'assurer que les règles de sécurité sont bien respectées.

## 2.2 Droits et devoirs de l'utilisateur :

La sécurité des moyens informatiques mis à la disposition impose à l'utilisateur :
- De respecter les consignes de sécurité et notamment les règles relatives à la définition et aux changements de mots de passe. Ce mot de passe ne doit correspondre ni à un mot, ni à un nom propre et ce, dans quelque langue que ce soit, et doit être gardé secret. Il doit comporter au minimum 6 caractères, choisis parmi des lettres, des chiffres et des caractères de ponctuation. Il peut être composé par exemple des premières lettres d'une phrase.
- De respecter la gestion des accès, en particulier ne pas utiliser les noms et mots de passe d'un autre utilisateur, ni chercher à connaître ces informations ;
- De garder strictement confidentiels ses mots de passe et ne pas les dévoiler à un tiers.
Si pour des raisons exceptionnelles et ponctuelles, un utilisateur se trouvait dans l'obligation de communiquer son mot de passe, il devra procéder, dès qu'il en a la possibilité, au changement de mot de passe ou en demander la modification à l'administrateur. Le bénéficiaire de la communication du mot de passe ne peut le communiquer à son tour à un tiers, ni l'utiliser en dehors de la circonstance exceptionnelle à l'origine de la communication.
- De verrouiller son poste de travail en cas d'absence et/ou d'utiliser les économiseurs d'écran avec mot de passe afin de préserver l'accès à son poste de travail ;
- D'avertir les administrateurs de tout dysfonctionnement constaté ;
- De ne pas installer, télécharger ou utiliser sur les matériels informatiques un logiciel et/ou un progiciel sans qu'une licence d'utilisation appropriée n'ait été souscrite par l'Université Paul Sabatier;
- De s'interdire d'accéder ou tenter d'accéder à des ressources informatiques pour lesquelles l'utilisateur ne bénéficie pas d'une habilitation expresse ; l'utilisateur doit limiter ses accès aux seules ressources pour lesquelles il est expressément habilité à l'exclusion de toute autre, même si cet accès est techniquement possible ;
- D'avoir une obligation de confidentialité et de discrétion à l'égard des informations et documents électroniques à caractère confidentiel disponibles dans le système d'information ;
- D'utiliser les ressources et les moyens informatiques prioritairement à des fins liées à leur formation et/ou à leur profession au sein de l'Université.
- De respecter l'architecture réseau de l'Université Paul Sabatier et de ne pas modifier sa configuration (connexion d'équipement réseau sur les prises murales) sauf accord préalable du correspondant réseau du bâtiment.

## 2.3 Droits et devoirs des administrateurs :

Les administrateurs ont le devoir d'assurer un bon fonctionnement des réseaux et des moyens informatiques. Ils ont le droit de prendre toutes dispositions nécessaires pour assumer cette responsabilité tout en respectant la déontologie professionnelle.
En particulier sur incident, les administrateurs peuvent être amenés avec l'autorisation du responsable de service, de laboratoire, de composante ou d'enseignement à examiner le contenu de fichiers ou boîtes aux lettres, de façon à obtenir suffisamment d'informations pour pallier les incidents de fonctionnement 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 ont l'obligation de préserver la confidentialité des informations privées qu'ils sont amenés à connaître dans ce cadre.
Les administrateurs sont autorisés, en cas de difficultés majeures, à prendre des mesures provisoires et conservatoires ou à arrêter des services réseaux.
Tout message transportant un virus sera détruit par les outils de sécurité informatiques sans que le destinataire et/ou l'émetteur puisse être informé.
Les utilisateurs peuvent demander l'aide des administrateurs pour faire respecter leurs droits.

### 2.4 Mesures de contrôle de la sécurité

Le système d'information ainsi que l'ensemble des moyens de communication peuvent donner lieu à surveillance et contrôle à des fins statistiques, de traçabilité, d'optimisation, de sécurité ou de détection des abus.

### 2.5 Sécurité du poste de travail

Un ordinateur propre à un département, laboratoire ou service, entre sur le réseau de l'Université sous contrôle d'un administrateur. Durant la vie du poste, l'utilisateur doit mettre en place un ou plusieurs dispositifs afin d'en assurer son intégrité. Les utilisateurs devront procéder à la mise à jour régulière des logiciels et/ou progiciels assurant la sécurité du système d'information et notamment des antivirus.
En cas de doute sur l'intégrité d'un poste de travail, le correspondant réseau du bâtiment peut le déconnecter. Le poste sera rebranché lorsque le correspondant réseau du bâtiment estimera qu'il ne portera pas atteinte à l'intégrité et à la sécurité du système d'information.

## 3. Usages des services Internet (Web, messagerie, forum)

Le réseau Internet n'est pas une zone de " non-droit " et se trouve soumis à l'ensemble des règles de droit.
L'utilisateur doit faire usage des services Internet dans le seul cadre de ses activités de formation et/ou professionnelles, dans le respect des principes généraux ainsi que dans le respect de la législation en vigueur.
Le téléchargement de fichiers, notamment de sons et d'images, depuis le réseau Internet est autorisé, dans le respect des droits de la propriété intellectuelle, mais doit correspondre à l'activité de l'Utilisateur dans l'Université.
Les messages électroniques permettent d'échanger des informations à vocation professionnelle liées à l'activité directe de l'Université Paul Sabatier. En toutes circonstances, les Utilisateurs doivent adopter un comportement loyal et digne et s'imposer le respect des lois et notamment celles relatives aux publications à caractère raciste, diffamatoire, injurieux, pornographique.
L'utilisateur doit faire preuve de la plus grande correction à l'égard de ses interlocuteurs dans les échanges électroniques.
La création d'espaces internes de discussion, de serveurs web ou de serveurs de transfert de fichiers est soumise à autorisation du Président de l'Université.

## 4. Propriété intellectuelle

L'utilisation des moyens informatiques implique le respect des droits de propriété intellectuelle de l'Université Paul Sabatier, de ses partenaires et plus généralement de tous tiers titulaires de tels droits.
Chacun doit :
- utiliser les logiciels dans les conditions des licences souscrites ;
- ne pas reproduire, copier, utiliser, diffuser, modifier et utiliser les logiciels, bases de données, pages web, textes, images, photographies ou autres créations protégées par le droit d'auteur ou un droit privatif sans avoir obtenu préalablement l'autorisation des titulaires de ces droits.

## 5. Respect de la loi informatique et libertés

Toutes les créations de fichiers comprenant des données nominatives, y compris lorsqu'elles résultent de croisement, d'interconnexion de fichiers préexistants, doit impérativement faire l'objet d'une déclaration et/ou demande d'avis préalable à la Commission Nationale de l'Informatique et des Libertés (CNIL).

## 6. Rappel des principales lois françaises

Il est rappelé que toute personne utilisant les ressources informatiques de l'Université Paul Sabatier est soumise à la législation française en particulier dans le domaine de la sécurité informatique :

- la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (cf. http://www.cnil.fr/);
- la législation relative à la fraude informatique (article 323-1 à 323-7 du Code pénal), (cf.http://www.legifrance.gouv.fr/citoyen/code.ow, puis "code pénal", "LIVRE II "chapitre III : Des atteintes aux systèmes de traitement automatisé de données")
- la législation relative à la propriété intellectuelle (cf.http://www.legifrance.gouv.fr/citoyen/code.ow, puis "code de la propriété intellectuelle")
- la loi du 04 août 1994 relative à l'emploi de la langue française (cf.http://www.culture.fr/culture/dglf/);
- loi du 20 juin 1992 relative au dépôt légal (cf.http://www.legifrance.gouv.fr/texteconsolide/ADEAS.htm )
- la législation applicable en matière de cryptologie (cf.http://www.telecom.gouv.fr/secur/index.htm).

## 7. Sanctions

Le non-respect des règles définies dans la présente Charte pourra entraîner la suppression immédiate du droit d'accès de l'utilisateur à tout ou partie du Système d'Information sur décision du Président de l'Université ainsi que, le cas échéant, des sanctions disciplinaires et /ou des poursuites judiciaires, civiles ou pénales.

UNIVERSITÉ TOULOUSE III – PAUL SABATIER
IUT de TARBES

1, rue Lautréamont
CS 41624
65016 TARBES

Tel. : 05 62 44 42 00
Fax : 05 62 44 42 01

www.iut-tarbes.fr