INSA DE TOULOUSE
REGLES D'UTILISATION DE L'INFORMATIQUE*

Le présent document définit les règles d'usage qui s'imposent à tout utilisateur des matériels, systèmes, logiciels ou réseaux informatiques (désignés ci-après par ressources ou moyens informatiques) de l'Institut National des Sciences Appliquées de Toulouse (INSAT). Est déclaré utilisateur toute personne qui fait usage des ressources informatiques de l'INSAT.

Il est avant tout un code de bonne conduite, afin d'instaurer un usage correct et loyal des moyens informatiques, dans le respect des lois et d'autrui.

1/ Engagements de l'INSA de Toulouse :

Le Centre des Services Numériques (CSN) de l'INSAT, dans la mesure de ses possibilités et des contraintes qui lui sont imposées :

- met à disposition des utilisateurs les matériels et les logiciels les plus adaptés à leurs besoins ;
- fournit un accès au réseau de l'INSAT et au travers de celui-ci à Internet via un compte informatique et éventuellement une adresse électronique ;
- maintient et sécurise au mieux le parc informatique, le réseau et les données ;
- assure la continuité du service offert.

2/ Devoirs des utilisateurs :

Bonne utilisation des ressources informatiques :

Chaque utilisateur est titulaire d'un compte (accès, mél...) personnel et confidentiel. L'utilisation des ressources et moyens informatiques est réservée aux travaux liés à l'enseignement, à la recherche et au fonctionnement de l'établissement. Toutefois, une utilisation culturelle est tolérée conformément à la note du Directeur « Usage raisonnable des ressources informatiques ».

L'utilisateur des moyens informatiques doit également se conformer aux consignes du CSN (par exemple : mise à jour de l'antivirus et du système) et signaler tout incident.

Il est tenu de respecter le matériel de l'INSAT et de ne pas modifier sa configuration (systèmes et logiciels) sauf accord préalable du CSN.

Tout matériel confié par l'institut devra être restitué au départ de l'utilisateur.

Respect de la sécurité :

Tout utilisateur s'engage à ne pas chercher à violer les mécanismes généraux de sécurité ni la confidentialité des données et à ne pas nuire aux autres usagers. Le réseau, les systèmes et les données ne doivent pas être mis en péril par des actes malveillants ou irréfléchis.

L'utilisateur devra également participer à la sécurité en utilisant son esprit critique : choix d'un mot de passe relativement complexe **à ne jamais divulguer**, manipulation des pièces jointes aux courriels...

Respect de la charte Renater :

Le réseau de l'INSAT étant raccordé à Internet via le réseau national Renater, les utilisateurs doivent également se conformer à la charte Renater :

http://www.renater.fr/IMG/pdf/charte_fr.pdf

Respect de la législation en vigueur :

L'utilisateur s'engage à respecter le cadre législatif et réglementaire applicable en droit, notamment droit de la personne, droits d'auteur et propriété intellectuelle.

3/ Données des utilisateurs :

Toutes les données (fichiers, courriels et publications notamment via le web) stockées sur des ressources informatiques de l'INSAT ou produites dans le cadre de l'enseignement, de la recherche et du fonctionnement de l'établissement y compris sur un matériel n'appartenant pas à l'INSAT, sont considérées, sauf mention contraire, à **caractère professionnel** et l'institut en est le propriétaire. En revanche, les données (fichiers, dossiers et courriels) avec la mention « privé » ou toute autre déclinaison explicite de ce terme, sont réputées personnelles. Quant aux publications sur Internet via les serveurs de l'INSAT, elles sont par nature professionnelles.

Les données à caractère professionnel doivent être systématiquement mises à disposition du chef d'établissement pour les enseignants-chercheurs ou du responsable hiérarchique pour les personnels qui quitte l'établissement. À défaut, elles seront transmises par un administrateur du CSN sur simple demande du responsable hiérarchique.

Les données des étudiants à caractère professionnel peuvent être mises à disposition de l'équipe enseignante par un administrateur du CSN sur simple demande pour assurer la continuité de la formation.

En cas de violation de ces règles ou mesures d'urgence afin de préserver les systèmes et les données, le CSN peut être amené à examiner le contenu de l'ensemble des fichiers de l'utilisateur. Les administrateurs doivent toujours respecter la confidentialité des informations dont ils auraient pu prendre, volontairement ou non, connaissance.

4/ Fichiers de journalisation (fichiers de suivi d'activité) :

Pour des nécessités d'investigation judiciaire, de sécurité, de maintenance et de gestion technique, les données de connexion, permettant d'identifier le poste ou l'utilisateur, sont conservées ainsi que l'historique de l'activité pendant le délai recommandé par la Commission Nationale de l'Informatique et des Libertés. Cela peut concerner les volumes échangés, l'identification des sites web consultés, la circulation des courriels, sans toutefois retranscrire les contenus.

5/ Sanctions pour non-respect des devoirs de l'utilisateur :

Les utilisateurs concernés pourront se voir interdire provisoirement par le CSN l'accès aux ressources informatiques après débat contradictoire ou en cas de force majeure. Ils pourront faire appel de cette décision auprès du Directeur de l'INSAT.

Les sanctions relevant de la procédure disciplinaire dans les établissements d'enseignement supérieur sont applicables.

Les sanctions civiles et pénales telles que prévues par les lois en vigueur sont applicables.