

# **INSA DE TOULOUSE**

## **REGLES D'UTILISATION DE L'INFORMATIQUE**<sup>\*</sup>

Le présent document définit les règles d'usage qui s'imposent à tout utilisateur des matériels, systèmes, logiciels et 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 de Ressources Informatiques (CRI) 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 éventuellement un compte et 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 éventuellement titulaire de comptes (accès, mél...) personnels et confidentiels. 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, dans des limites raisonnables, permettant d'éviter toute consommation abusive des ressources.

L'utilisateur des moyens informatiques doit se conformer aux consignes du CRI (par exemple : mise à jour de l'antivirus et du système) et signaler tout incident. Il est également tenu de respecter le matériel de l'INSAT et de ne pas modifier sa configuration (systèmes et logiciels) sauf accord préalable du CRI.

#### *Respect de la sécurité :*

Tout signataire du présent document 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 utilisateurs. 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/Services/Procedures/DeontologieUtilisation.htm>

### *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 :

Les utilisateurs sont responsables de leurs données. Celles-ci sont de nature professionnelle et peuvent être transmises au responsable hiérarchique sur simple demande pour assurer la continuité du service. Seules les données explicitement désignées comme personnelles (présentes dans un dossier dénommé « privé ») ne seront pas divulguées.

En cas de violation de ces règles ou mesures d'urgence afin de préserver les systèmes et les données, le CRI 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 de maintenance, de gestion technique et de sécurité, 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 CRI 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.

## DÉCLARATION

Je, soussigné(e)

en qualité de :      ☐ personnel INSAT                      ☐ étudiant INSAT  
                                 ☐ autre (à préciser) :

déclare avoir pris connaissance de l'intégralité de ce document et m'engage à en respecter les obligations.

Lu et approuvé  
Toulouse, le

Signature :