

REGLEMENT D'UTILISATION DES MOYENS INFORMATIQUES DES COMPOSANTES, DEPARTEMENTS
ET TOUS SERVICES DE L'ETABLISSEMENT

Adopté au Conseil d'Administration du 19 septembre 1997

Modifié au Conseil d'Administration du 20 janvier 1998

Article 1 - DOMAINE D'APPLICATION

Ces règles s'appliquent à toute personne utilisant les systèmes informatiques de l'UJF et les systèmes informatiques auxquels il est possible d'accéder à partir de l'établissement. Les activités spécifiques liées à l'administration des systèmes et des réseaux par les administrateurs désignés relèvent des règles détaillées en article 6. On appelle "Utilisateur" toute personne, quelque soit son statut (étudiant, enseignant, chercheur, ingénieur, administratif, personnel temporaire, stagiaire, ...) appelée à utiliser les ressources informatiques et réseaux de l'établissement.

Article 2 - CONDITIONS D'ACCES AUX RESSOURCES INFORMATIQUES ET RESEAUX

L'utilisation des moyens informatiques et réseaux de l'UJF doit être limitée à des activités de recherche, d'enseignement, de gestion ou de vie universitaire. Sauf autorisation préalable, ils ne peuvent pas être utilisés pour des activités faisant l'objet d'un financement extérieur. L'utilisateur ne peut pas connecter un équipement informatique aux ressources informatiques et réseaux de l'établissement sans autorisation préalable. L'utilisateur doit respecter les modalités de raccordement des matériels aux réseaux de communication telles qu'elles lui sont précisées par le responsable des moyens informatiques. Ces raccordements ne pourront pas être modifiés sans autorisation préalable. Le droit d'accès à un système informatique est personnel et incessible. L'utilisateur est responsable de l'utilisation des ressources informatiques (locales ou distantes) effectuée à partir de son droit d'accès. Le droit d'accès est temporaire ; il est retiré dans les cas suivants :

- ✓ La fonction de l'utilisateur ne le justifie plus
- ✓ Non-respect du présent règlement

En conséquence

- ✓ Si un utilisateur chercheur quitte de manière définitive un laboratoire de l'UJF,
- ✓ Si un utilisateur administratif ou technique quitte de manière définitive son service d'affectation,

Cet utilisateur doit prévenir son responsable des ressources informatiques (administrateur système) pour l'informer de son départ, afin que celui-ci lui retire son droit d'accès. (Additif du Conseil d'Administration du 20 janvier 1998)

Article 3 - RESPECT DU CARACTERE CONFIDENTIEL DES INFORMATIONS

Les utilisateurs ne doivent pas tenter de lire ou de copier les fichiers d'un autre utilisateur sans son autorisation. Les informations contenues dans les fichiers d'un utilisateur sont privées même si les fichiers sont "physiquement" accessibles. Les utilisateurs doivent s'abstenir de toute tentative d'interception de communications privées entre utilisateurs. 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). Les utilisateurs doivent s'abstenir de toute tentative de s'approprier ou de déchiffrer le mot de passe d'un utilisateur, de modifier, copier ou détruire des fichiers d'un autre utilisateur, et de limiter ou d'interdire l'accès aux systèmes informatiques d'un utilisateur autorisé.

Article 4 - RESPECT DES DROITS DE PROPRIETE

Les utilisateurs doivent s'abstenir de faire des copies de tout logiciel autre que ceux du domaine public. Les copies de sauvegardes sont la seule exception.

Article 5 - RESPECT DES PRINCIPES DE FONCTIONNEMENT DES SYSTEMES INFORMATIQUES

Les utilisateurs acceptent les droits de l'administrateur, tels qu'il sont définis en article 6.

• **Article 5.1 - Sécurité informatique**

Les utilisateurs sont tenus de participer à la sécurité du système (choix de bon mots de passe, protection de son espace de fichier, signaler tout problème de sécurité, ...) Les utilisateurs ne doivent pas effectuer de manoeuvre qui aurait pour objet de méprendre les autres utilisateurs sur leur identité. L'utilisateur doit respecter les procédures d'authentification en vigueur de façon à ce que les actions qu'il mène au sein des systèmes soient identifiables. Les utilisateurs ne doivent pas effectuer d'expérimentation sur la sécurité des systèmes informatiques et réseaux, ni sur les virus informatiques sans autorisation préalable. Le développement, l'installation, ou la simple détention d'un programme ayant les propriétés décrites ci-dessous sont également interdits :

- ✓ Programmes cherchant à contourner la sécurité d'un système
- ✓ Programmes contournant les protections des logiciels

Tout utilisateur d'un réseau informatique s'engage à ne pas effectuer d'opérations qui pourraient avoir pour conséquence :

- ✓ d'interrompre le fonctionnement du réseau ou d'un système connecté au réseau;
- ✓ d'accéder aux informations privées d'autres utilisateurs sur le réseau;
- ✓ de modifier ou de détruire des informations sur un des systèmes connectés au réseau;
- ✓ de nécessiter la mise en place de moyens humains ou techniques supplémentaires pour son contrôle.

• **Article 5.2 Gestion des ressources**

Les utilisateurs doivent respecter les règles et procédures mises en place pour l'acquisition et la sortie des données sur les machines de l'établissement. Ils respecteront les procédures et restrictions d'acquisition/extraction des données à partir des supports électroniques. Ceci concerne principalement les accès téléinformatiques et les supports amovibles (disquettes, bandes, etc...). Les utilisateurs ne doivent utiliser que les ressources pour lesquelles ils ont eu autorisation d'usage. Ceci est valable aussi bien pour les points d'accès, que pour des périphériques (imprimantes, traceurs, ...) Les utilisateurs sont tenus de participer à l'exploitation des ressources en se conformant aux

directives d'exploitation précisant les modalités d'accès et de partage de ces ressources. Le développement, l'installation, ou la simple détention d'un programme saturant les ressources (informatiques et/ou réseaux) sont également interdits.

• **Article 5.3 Respect d'un comportement correct**

Un utilisateur ne doit pas utiliser les systèmes informatiques pour harceler d'autres utilisateurs par des communications non souhaitées par les tiers ou pour afficher/diffuser des informations illégales.

Il est rappelé que des lois plus générales s'appliquent pour des informations ou messages :

- ✓ à caractère injurieux,
- ✓ à caractère pornographique,
- ✓ à caractère diffamatoire,
- ✓ d'incitation au racisme,
- etc

Article 6 - DROITS ET DEVOIRS DE L'ADMINISTRATEUR D'UNE RESSOURCE INFORMATIQUE

• **Article 6.1 Les devoirs de l'administrateur**

Les administrateurs sont responsables de la qualité de service des ressources qu'ils ont en charge. Les administrateurs doivent appliquer la politique de sécurité informatique définie par l'établissement et donc appliquer les recommandations fournies par le responsable sécurité de l'établissement. L'administrateur est tenu de prévenir le responsable sécurité de l'établissement lors de détections de problèmes de nature sécuritaire sur les équipements dont il est le responsable. Lorsque l'administrateur détecte (ou est informé par un utilisateur) de problèmes liés à la sécurité informatique, il doit avertir le responsable sécurité de l'établissement. Ce dernier en fonction de la nature des problèmes et son degré de gravité déclenche un audit de sécurité avec l'administrateur. L'administrateur doit respecter la confidentialité des fichiers utilisateurs, des courriers et des sorties imprimantes auxquels il peut être amené à accéder lors de ses tâches d'administration et/ou lors d'audit de sécurité. (Notion de secret professionnel)

• **Article 6.2 Les droits de l'administrateur**

L'administrateur est responsable de la distribution et du retrait des droits d'accès. Les administrateurs doivent faire respecter les droits et responsabilités des utilisateurs présents sur leurs ressources. L'administrateur se réserve le droit de prendre toutes dispositions nécessaires pour assumer ses responsabilités et permettre le fonctionnement optimal des ressources informatiques qu'il a en charge. L'administrateur peut prendre des mesures "conservatoires" (arrêts de travaux, suppression de droits d'accès, verrouillage de fichiers, ...) en vue de :

- ✓ Arrêter un engorgement de ses ressources
- ✓ Figurer un état lors de problèmes liés à la sécurité des systèmes informatiques

L'administrateur peut :

- ✓ accéder à des fichiers ou des courriers en vue de réaliser un diagnostic, une correction d'un problème et/ou s'assurer du bon fonctionnement des ressources qu'il a en charge.
- ✓ examiner des données utilisateurs en vue d'assurer la bonne marche du système qu'il a en charge et/ou de s'assurer du bon respect du règlement de la part des utilisateurs.
- ✓ contrôler la bonne utilisation des ressources et prendre des décisions pouvant affecter l'espace fichier ou les travaux lancés par un utilisateur.
- ✓ surveiller en détail les sessions de travail d'un utilisateur soupçonné de non-respect du présent règlement.

Tout utilisateur n'ayant pas respecté le règlement énoncé ci-dessus est passible de poursuites :

- internes à l'établissement
- pénales pour les infractions relevant du Nouveau Code Pénal.

NOM D'USAGE : _____ PRENOM : _____

NOM DE NAISSANCE: _____ DATE DE NAISSANCE : _____

Etablissement payeur (UJF, INPG, CNRS, INSERM...) : _____

Statut (permanent, contractuel, stagiaire.....) : _____ Date de départ prévu : _____

Adresse électronique : _____

Affectation (service/composante....) : _____

Mention à porter à la main : « Je soussigné(e) (Nom, Prénom) atteste avoir lu le présent règlement et m'engage à le respecter. »

Je soussigné(e) : _____

Fait à _____, le _____ Signature : _____