INSTRUCTION D'UTILISATION DES MOYENS INFORMATIQUES

Mise à jour en conformité avec le règlement intérieur de l'établissement – avril 2008

Préambule

La présente instruction a pour objet de définir les règles d'utilisation des moyens informatiques de l'Institut polytechnique de Grenoble, en particulier de préciser les responsabilités des utilisateurs, conformément à la réglementation et afin de permettre un usage normal et optimal des ressources informatiques et des services Internet employés dans l'établissement.

1. CHAMP D'APPLICATION

Ces règles s'appliquent à toute personne autorisée à utiliser les moyens informatiques de l'Institut, y compris les moyens informatiques mutualisés ou externalisés, et s'étendent aux réseaux extérieurs accessibles par l'intermédiaire des réseaux de l'établissement : TIGRE, RENATER et INTERNET.

Toute personne devient utilisateur d'un système informatique à partir du moment où elle a reçu de l'établissement, un moyen d'accès (identifiant/mot de passe, carte magnétique ou à puce, …).

L'utilisation du réseau RENATER est régie par une "Charte d'usage et de sécurité" que l'établissement s'est engagé à respecter.

2. RESPECT DE LA LEGISLATION

La quantité et la facilité de circulation des informations et des contenus sur Internet ne doivent pas faire oublier la nécessité de respecter la législation. Internet n'est pas une zone de non-droit.

Ce rappel non exhaustif des règles de droit principalement concernées par l'utilisation des moyens informatiques de l'établissement vise le double objectif de sensibiliser l'utilisateur à leur existence et à leur respect et de renforcer ainsi la prévention d'actes illicites.

Outre l'atteinte aux principes généraux de l'éducation nationale, dont en particulier les principes de neutralité religieuse, philosophique, politique et commerciale, sont également (mais pas exclusivement) interdits et pénalement sanctionnés :

- l'atteinte à la vie privée d'autrui ;
- la diffamation et l'injure ;
- la provocation de mineurs à commettre des actes illicites ou dangereux, le fait de favoriser la corruption d'un mineur, l'exploitation à caractère pornographique de l'image d'un mineur, la diffusion de messages à caractère violent ou pornographique susceptibles d'être perçus par un mineur ;
- l'incitation à la consommation de substances interdites ;
- la provocation aux crimes et délits et la provocation au suicide, la provocation à la discrimination à la haine notamment raciale, ou à la violence ;
- l'apologie de tous les crimes, notamment meurtre, viol, crime de guerre et crime contre l'humanité ; la négation de crimes contre l'humanité.

De même tout ce qui concerne les droits de propriété :

- les copies de logiciels sous licence pour quelque usage que ce soit, hormis une copie de sauvegarde dans les conditions prévues par le code de la propriété intellectuelle et hormis les autorisations exprimées dans la licence ;
- la contrefaçon de marque ;
- la reproduction, représentation ou diffusion d'une œuvre de l'esprit (par exemple : extrait musical, photographie, extrait littéraire,...) ou d'une prestation de droits voisins (par exemple : interprétation d'une œuvre musicale par un artiste, phonogramme, vidéogramme, programme d'une entreprise de communication audiovisuelle) en violation des droits de l'auteur, du titulaire des droits voisins et/ou du titulaire des droits de propriété intellectuelle ;

- l'usage des ressources pédagogiques diffusées sous format numérique doit donc être limité à un usage personnel en respectant les droits de propriété intellectuelle (pas de modification sans autorisation de l'auteur) et les droits de diffusion (pas de copie sous quelque forme que ce soit hormis la copie de sauvegarde permettant le travail personnel et pas de diffusion auprès de tiers).

3. CONDITIONS D'ACCES AU SYSTEME D'INFORMATION

3.1. RESPECT DES PROCEDES D'AUTHENTIFICATION

Chaque utilisateur se voit attribuer des moyens d'accès au Système d'Information en fonction des ses besoins : identifiant/mot de passe, carte magnétique, carte à puce… Il est responsable de la confidentialité des informations stockées ou transmises au moyen des ressources informatiques.
Les moyens d'accès à un système informatique sont personnels et incessibles. Ils ne doivent pas être communiqués ou remis à un tiers. Chaque utilisateur est responsable de l'utilisation qui en est faite.
Les utilisateurs ne doivent pas utiliser de compte autre que ceux qui leur ont été attribués. Ils ne doivent pas non plus effectuer de manœuvre qui aurait pour but de tromper sur leur identité ou sur celle d'autres utilisateurs. La conception d'un programme ayant de telles propriétés est également interdite sans autorisation préalable.
Les utilisateurs ne doivent pas laisser leur poste de travail en libre accès (ils doivent fermer ou bloquer la session en cours, fermer à clé leur bureau, …).
Les mots de passe seront choisis pour être difficiles à deviner.

3.2. UTILISATION DES MOYENS INFORMATIQUES

Les moyens informatiques mis à disposition de ses personnels et usagers par l'établissement ont pour objet exclusif d'être le support de ses missions. Sauf autorisation préalable délivrée par l'administrateur de l'Institut, ces ressources ne peuvent être employées en vue d'une utilisation ou de la réalisation de projets ne relevant pas des missions de l'Institut ou des missions confiées aux utilisateurs.

Chacun veillera à protéger les matériels mis à sa disposition contre le vol et les dégradations (chutes, liquides, …).

Services Internet (Web, messagerie, forum, téléchargement, chat, ...)

L'utilisateur doit faire usage des services Internet dans le cadre exclusif de ses activités professionnelles. Une utilisation ponctuelle et raisonnable des services internet, pour un motif personnel, dans le respect de la législation et sans mettre en cause l'intérêt ou la réputation de l'établissement, est tolérée.

L'Institut se réserve le droit de filtrer l'accès à certains sites ou à certains services.

Les outils de courrier électronique

L'utilisateur doit faire preuve de vigilance vis-à-vis des informations reçues (désinformation, virus informatique, tentative d'escroquerie, chaînes, …).

Un usage ponctuel et raisonnable dans le cadre des nécessités de la vie courante et familiale est toléré à condition qu'il n'affecte pas le trafic normal des messages professionnels. Tout message à caractère privé, reçu ou émis, doit comporter une mention particulière nommée «**privé**» indiquant le caractère privé dans la zone «objet» ou «sujet» du message. À défaut, le message sera réputé professionnel sauf s'il est stocké dans un espace privé de données.

L'Institut ne garantit pas que le service de messagerie soit exempt de toute interruption, retard, incident de sécurité ou erreur, et avise ses utilisateurs de l'emploi d'outils de contrôle (filtres antivirus, antispam, blocage de certains types de pièces jointes, limitation de la taille des messages, etc.).

Stockage

L'utilisation des ressources doit être rationnelle et loyale afin d'en éviter la saturation. L'utilisateur doit donc s'efforcer à n'occuper que la quantité d'espace disque qui lui est strictement nécessaire pour son travail.

Toutes les informations ne se trouvant pas dans un espace de données nommé «**privé**» sont réputées professionnelles. L'utilisateur est averti que les outils de sauvegarde ou récupération des données ne permettent pas tous de distinguer les données privées. Il appartient à l'utilisateur, lors de son départ définitif du service ou de l'établissement, de récupérer le contenu de son espace «**privé**» et le supprimer

des machines de l'établissement ; sinon, la responsabilité de l'établissement ne pourra être engagée quant à leur conservation.

Raccordement au réseau

Le raccordement de tout équipement au réseau y compris par les technologies sans fil est soumis à l'autorisation du responsable informatique du site.
La connexion au réseau de tout équipement informatique n'appartenant pas à l'établissement n'est possible qu'en utilisant exclusivement le réseau sans fil ou les prises réseaux réservées à cet effet. Les utilisateurs devront se soumettre à la procédure mise en place par le service informatique local (identification ; configuration et salubrité de l'ordinateur). Il est interdit de débrancher les connexions électriques ou informatiques des matériels mis à disposition par l'établissement pour y substituer un équipement personnel.

Il est rappelé que les services informatiques n'ont pas pour mission de maintenir les postes personnels des utilisateurs.

Utilisation des réseaux informatiques

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

- d'interrompre ou de perturber le fonctionnement du réseau ou d'un système connecté au réseau,
- d'accéder à des 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.

Installation de logiciels et de périphériques

L'installation de tout logiciel et de tout périphérique (y compris par des technologies sans fil) sur le poste de travail fourni par l'Institut doit faire l'objet, par tout moyens, d'une demande d'autorisation auprès du responsable des moyens informatiques de l'entité qui valide leur bon fonctionnement et leur intégration dans le système d'informations A défaut, une régularisation doit intervenir dans les plus brefs délais *a posteriori*.

L'utilisateur ne devra en aucun cas :

- contourner les restrictions d'utilisation d'un logiciel ;
- développer des programmes constituant ou s'apparentant à des virus, vers, ...

3.3. ENGAGEMENT DE L'UTILISATEUR

L'utilisateur s'engage

- à appliquer les recommandations de sécurité de l'établissement ;
- à signaler sans délai toute perte de ses moyens d'accès (mot de passe, carte, …) ;
- à signaler sans délai toute tentative de violation de son compte ou anomalie dans son environnement de travail ;
- à ne pas lire, ni copier, ni tenter de lire ou copier les fichiers d'un autre utilisateur sans son autorisation, verbale ou écrite ;
- à ne pas intercepter ou tenter d'intercepter les communications entre utilisateurs ;
- à ne pas harceler un individu à l'aide d'outils électroniques.

Les échanges électroniques (courriers, forums de discussion, etc.) se doivent de respecter la correction normalement attendue dans tout type d'échange tant écrit qu'oral.

4. SURVEILLANCE DES SYSTEMES SUR LES LIEUX DE TRAVAIL

4.1. INFORMATIQUE ET LIBERTES

La création de tout traitement de données à caractère personnel doit respecter la loi informatique et libertés ; il doit être déclaré préalablement à sa mise en œuvre auprès du Correspondant Informatique et Libertés (CIL) désigné par l'Institut à la Commission Nationale Informatique et Libertés. Un acte réglementaire définit, pour chacun de ces traitements, les conditions d'exploitation et de sécurisation de ces traitements et des données traitées ou en résultant et les conditions permettant aux usagers d'exercer leur droit d'accès aux informations les concernant.

La collecte, le traitement, la conservation de données à caractère personnel et leur transmission éventuelle à des tiers doit s'effectuer de manière loyale. Les données ne peuvent être collectées et traitées à l'insu de la personne concernée : elle doit être informée de l'identité et du lieu d'établissement de la personne qui traite les données, du caractère obligatoire ou facultatif de ce traitement, des destinataires des informations ainsi que toute information nécessaire à l'exercice de ces droits.

Les principes à respecter sont :

- la pertinence et l'exactitude des données au regard des finalités poursuivies,
- le consentement individuel à la collecte de données,
- le droit d'accès, de rectification et d'opposition,
- la protection adaptée aux risques présentés par le traitement sur le plan technique et le plan organisationnel.

4.2. LES FICHIERS DE JOURNALISATION

Ces fichiers permettent d'identifier et d'enregistrer toutes les connexions ou tentatives de connexion au système d'information ainsi que les traces de l'activité sur celui-ci.
Ils constituent une mesure de sécurité conformément à la législation et sont conservés un an, à destination de l'autorité judiciaire en cas de besoin de recherche, de constatation et de poursuite des infractions pénales.

4.3. CONTROLE DES PAGES WEB HEBERGEES

L'Institut se réserve le droit de contrôler le contenu et l'accès à toute page Web hébergée sur ses serveurs.

5. LES RESPONSABLES ET ADMINISTRATEURS SYSTEMES ET RESEAU

Comme tout utilisateur, ces personnels (informaticiens, enseignants ou chercheurs gérant des machines, ainsi que tout prestataire externe), s'engagent à respecter cette instruction. Ils sont tenus au secret professionnel et ne doivent pas divulguer les informations à caractère privé qu'ils auraient été amenés à connaître dans le cadre de leurs fonctions. Leur autorité hiérarchique ne peut les contraindre à cette divulgation que dans le cadre d'une commission rogatoire.

Pour garantir l'intégrité du Système d'Information, ils peuvent être amenés à prendre des mesures d'urgence, dans le respect de la législation.

6. DISPONIBILITE DU SERVICE

Une commission de concertation entre les informaticiens et les utilisateurs se réunit pour évaluer le bon fonctionnement des systèmes d'informations.

L'Institut s'efforce dans la mesure du possible de maintenir accessible le service qu'il propose de manière permanente, mais n'est tenu à aucune obligation d'y parvenir. Des interruptions ponctuelles ou totales de service à l'initiative de l'Institut ou d'organismes gouvernementaux (Renater, Haut Fonctionnaire de Défense, …) peuvent se produire pour des raisons de maintenance, de sécurité informatique ou pour toutes autres raisons, sans que l'établissement puisse être tenu pour responsable des conséquences de ces interruptions aussi bien pour l'utilisateur que pour tout tiers. L'Institut essaiera, dans la mesure du possible, de tenir les utilisateurs informés de ces interruptions.

7. SANCTIONS

Tout utilisateur n'ayant pas respecté cette instruction est susceptible de poursuites devant la section disciplinaire du Conseil d'administration de l'Etablissement (décret 92-657 du 13 juillet 1992 relatif aux procédures disciplinaires dans les établissements publics d'enseignement supérieurs…) et/ou pénales (articles 323-1 et suivants du Code Pénal).

Ces règles doivent être portées à la connaissance des utilisateurs par tout moyen, y compris affichage dans les locaux.

Le responsable hiérarchique a le droit de demander la fermeture d'un compte dès qu'une infraction aux règles ci-dessus est constatée.

8. PRINCIPALES REFERENCES REGLEMENTAIRES

8.1. INFRACTIONS PREVUES PAR LE NOUVEAU CODE PENAL

Crimes et délits contre les personnes

Atteintes à la personnalité : (Respect de la vie privée art. 9 du code civil)

- Atteintes à la vie privée (art. 226-1 al. 2 ; 226-2 al. 2, art.432-9 modifié par la loi nº2004-669 du 9 juillet 2004) ; atteintes à la représentation de la personne (art. 226-8)
- Dénonciation calomnieuse (art. 226-10)
- Atteinte au secret professionnel (art. 226-13)
- Atteintes aux droits de la personne résultant des fichiers ou des traitements informatiques (art. 226-16 à 226-24, issus de la loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés

Atteintes aux mineurs : (art. 227-23 ; 227-24 et 227-28).

- Loi 2004- 575 du 21 juin 2004 (LCEN)

Crimes et délits contre les biens

- Escroquerie (art. 313-1 et suite)
- Atteintes aux systèmes de traitement automatisé de données (art. 323-1 à 323-7 modifiés par la loi nº 2004-575 du 21 juin 2004).

Cryptologie

- Art. 132-79 (inséré par loi nº 2004-575 du 21 juin 2004 art. 37)

8.2. INFRACTIONS DE PRESSE (LOI 29 JUILLET 1881, MODIFIEE)

- Provocation aux crimes et délits (art.23 et 24)
- Apologie des crimes contre l'humanité, apologie et provocation au terrorisme, provocation à la haine raciale, « négationnisme » contestation des crimes contre l'humanité (art. 24 et 24 bis)
- Diffamation et injure (art. 30 à 33)

8.3. INFRACTION AU CODE DE LA PROPRIETE INTELLECTUELLE

- Contrefaçon d'une œuvre de l'esprit (y compris d'un logiciel) (art. 335-2 modifié par la loi nº 2004-204 du 9 mars 2004, art. 34 - et art. 335-3)
- Contrefaçon d'un dessin ou d'un modèle (art. L521-4 modifiée par la loi nº 2004-204 du 9 mars 2004, art. 34)
- Contrefaçon de marque (art. L716-9 - modifié par la loi nº 2004-204 du 9 mars 2004, art.34 -et suivants)

Il est rappelé que cette liste n'est qu'indicative et que la législation est susceptible d'évolution.