CHARTE DU BON USAGE
DES RESSOURCES INFORMATIQUES DE L'INALCO

La présente charte a pour objet de définir les règles d'utilisation des moyens informatiques mis à la disposition des étudiants.

1. Introduction

Ce texte est avant tout un code de bonne conduite. Il a pour objet de préciser la responsabilité des étudiants en accord avec la législation en vigueur afin d'instaurer un usage correct des ressources informatiques et des services internet. Il informe les étudiants des sanctions encourues en cas de non observation des dispositions légales et réglementaires. Cette Charte est mise à la disposition des étudiants lors de l'inscription.

1.1. Notion de délits informatiques

Les délits informatiques sont principalement de quatre types : a/ intrusion sur un ordinateur ou sur un réseau ; b/ réalisation, utilisation ou diffusion d'une copie illicite de logiciels ; c/ vol de fichiers informatiques ; d/ emprunt de l'identité d'un tiers.

1.2. Existence d'un Droit de l'Informatique (sanctions)

Il est rappelé qu'en plus des poursuites administratives, des poursuites judiciaires peuvent être engagées par le Président de l'INALCO ou par toute victime, tant sur le plan pénal qu'en réparation du préjudice subi.

NUL N'EST CENSE IGNORER LA LOI

Pour mémoire, les principaux textes de référence en matière informatique sont : · la loi « informatique et libertés » de janvier 1978 ; · la loi sur l'accès aux documents administratifs de juillet 1978 ; · la loi sur la protection des logiciels de 1985 ;· la loi relative à la fraude informatique du 5 janvier 1988 ;· la loi Hadopi ou « création et internet » du 12 juin 2009 ;· la charte déontologique d'utilisation du réseau RENATER qui peut être téléchargée à l'adresse http://www.renater.fr/Telechargement/charte_v12.pdf

2. Quelques définitions

Ressources informatiques : les ressources informatiques de l'INALCO sont constituées de serveurs, stations de travail, micro-ordinateurs, logiciels, données... appartenant ou utilisés à l'INALCO et de réseaux internes ou externes liés à l'institut (RAP, RENATER...).
Services internet : les moyens d'échange et d'informations diverses mis à disposition par des serveurs locaux ou distants. Administrateur : la personne physique ayant la responsabilité de l'une des ressources informatiques de l'INALCO.

3. Règles d'usage

L'utilisation des moyens informatiques et l'usage des services Internet ainsi que du réseau géré par l'INALCO sont autorisés aux étudiants dans le cadre exclusif de leurs études et des activités qu'ils exercent à l'INALCO. Tout étudiant est responsable de l'utilisation qu'il fait des ressources informatiques et s'engage à ne pas effectuer d'opérations qui pourraient avoir des conséquences néfastes sur l'intégrité de l'outil informatique, sur le fonctionnement normal des réseaux et sur les relations internes et externes de l'établissement.
L'utilisation de logiciels non fournis par l'établissement ne peut être tolérée. Les étudiants sont informés que les administrateurs-système appartenant au service informatique ont la possibilité technique d'accéder à toutes les informations disponibles sur les serveurs. En cas d'actes graves pouvant compromettre la sécurité du système ou le droit des personnes, par exemple, les administrateurs-système pourront être autorisés par le Président de l'INALCO, dans le cadre prévu par la loi, à utiliser tout moyen disponible pour faire cesser ces actes interdits par la loi et susceptibles de compromettre le bon fonctionnement de l'INALCO.

4. Règles de sécurité

Tout étudiant est responsable de l'utilisation qu'il fait des ressources informatiques de l'INALCO à partir des comptes et des matériels mis à sa disposition. L'utilisateur peut être tenu de fournir à l'administrateur des informations permettant son identification et de l'informer de toute modification de ces informations. La fourniture d'informations intentionnellement erronées constitue une faute grave.
Le droit d'accès à une ressource informatique est personnel, incessible et peut être temporaire. Il est soumis à l'autorisation de l'administrateur et assorti de moyens d'identification. Il peut être retiré si les conditions d'accès ne sont plus respectées ou si le comportement de l'utilisateur est contraire à la Charte. Les moyens d'accès ou d'identification (clef, carte magnétique, code, mot de passe, etc...) sont remis à titre personnel et sont incessibles. Ils ne peuvent être prêtés, donnés ou vendus à des tiers et sont rendus en fin d'activité.
L'utilisateur doit prévenir l'administrateur de tout accès frauduleux ou tentative d'accès aux ressources qu'il utilise. Il est responsable de la protection de ses fichiers et de l'accès à ses données. Les étudiants ne doivent pas tenter de lire, de copier, de divulguer ou de modifier des informations (fichiers...) d'un autre utilisateur sans y avoir été explicitement autorisés. Il faut noter que la capacité d'accéder à une information n'implique pas que l'accès soit effectivement autorisé.
La possession, l'installation ou le développement de programmes mettant en cause l'intégrité des systèmes informatiques sont interdits: · programme pour contourner la sécurité ; · programme saturant les ressources informatiques ; · programme-virus ou générateur de virus ; · programme contournant la protection des logiciels.
La possession, l'utilisation ou le développement de programmes cherchant à s'approprier ou à déchiffrer le mot de passe d'un autre utilisateur sont interdits.

5. Protection des droits de la personne

Tout étudiant utilisateur des ressources informatiques de l'INALCO s'engage notamment à ne pas diffuser de messages, de logiciels ou de documents électroniques : · contenant des propos injurieux, diffamatoires ou pouvant porter atteinte à l'honneur ou à la réputation d'un individu, d'une institution ou d'une personne morale ; · à caractère raciste, xénophobe ou révisionniste ; · violant ou incitant à violer les dispositions protégeant les mineurs ;

6. Protection de la propriété intellectuelle

L'utilisateur ne doit pas reproduire, télécharger, copier, diffuser, modifier ou utiliser les logiciels, bases de données, pages web, 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.

7. Sanctions éventuelles

7.1. Sanctions internes

La tentative d'accès illicite à une ressource informatique de la part d'un utilisateur peut entraîner la suppression de tout accès à l'une ou l'autre des ressources informatiques de l'INALCO.
Le droit d'accès peut être refusé à toute personne ayant contrevenu à la Charte. Les fautes peuvent être sanctionnées disciplinairement dans le cadre des peines prévues par le statut particulier de l'utilisateur.

7.2. Sanctions pénales

L'INALCO est tenue par la loi de signaler toute violation des lois dûment constatée. Toute personne ayant connaissance d'un délit relatif à l'informatique est tenue de le dénoncer dans les formes prévues par le Code de Procédure Pénale. Quelques exemples de délits et peines sont donnés dans l'annexe jointe.

7.3. Sanctions civiles

Les auteurs d'agissements contraires à la loi peuvent être condamnés à des réparations en dommages-intérêts aux victimes ayant subi des préjudices.

Annexe

PRINCIPALES DISPOSITIONS SE RAPPORTANT A LA SECURITE DES SYSTEMES INFORMATIQUES ET A LA PROTECTION DES PERSONNES

La CNIL (Commission Nationale de l'Informatique et des Libertés)
Elle a été mise en place par la loi du 6 janvier 1978 sur l'informatique, les fichiers et les libertés. Exemple de sanctions pour infraction à la loi (Art.226-16 du Nouveau Code Pénal) : jusqu'à 5 ans d'emprisonnement et 200 000 francs d'amende.

Les atteintes à la propriété intellectuelle : la contrefaçon
L'article 335-2 du Code de la Propriété Intellectuelle interdit à l'utilisateur d'un logiciel toute reproduction autre que celle d'une copie de sauvegarde. Toute autre copie est considérée comme une contrefaçon et constitue un délit. Sanctions prévues : jusqu'à 3 ans d'emprisonnement et 300 000 euros d'amende.

Les atteintes aux systèmes de traitement automatisé de données
Sanctions prévues : Accès frauduleux (Art.323-3 du Nouveau Code Pénal) : jusqu'à 5 ans d'emprisonnement et 75 000 euros d'amende. Peines complémentaires (Art.323-5): interdiction d'exercer dans la fonction publique ou certaines activités professionnelles.

La violation des secrets
Sanctions prévues: Secret de fabrique (Art.621-1 de la Propriété Individuelle): 2 ans de prison et 30 000 euros d'amende. Se rappeler que les dommages-intérêts pour les victimes de tels agissements sont parfois supérieurs à une amende pénale. (Exemple: des étudiants de l'IUT de Toulouse ont été condamnés en 1988 à 8 mois d'emprisonnement avec sursis, 5000 francs d'amende et 70 000 francs de dommages-intérêts aux victimes).

RAPPEL DE QUELQUES RECOMMANDATIONS ELEMENTAIRES

1. Tout compte utilisateur doit être protégé par un mot de passe.
2. Un mot de passe doit être changé régulièrement et ne pas être trivial.
3. Un mot de passe ne doit pas être affiché même si le poste de travail est partagé par plusieurs personnes travaillant sur le même bureau.
4. Un mot de passe ne doit jamais être donné à un tiers et un compte ne doit jamais être prêté.
5. Des supports informatiques (disquettes, bandes, disques durs, CD rom..) ne doivent jamais être abandonnés dans un bureau ouvert.
6. L'utilisateur doit s'assurer de l'absence de virus lors de l'utilisation ou de la copie de tout fichier ou programme quelle qu'en soit l'origine.
7. L'utilisateur doit veiller de façon permanente à réglementer l'accès et le partage de ses fichiers.
8. Toute session de travail doit être terminée proprement. En cas d'incident ou de fin anormale, l'administrateur doit être prévenu immédiatement.
9. Il est conseillé de changer le mot de passe après la présentation publique d'une application.
10. Des sessions multiples et inactives sont à proscrire.
11. Un poste de travail ne doit jamais être quitté lorsqu'une session est en cours.
12. Toute modification de paramétrage d'une connexion à un réseau ne peut être effectuée qu'avec l'accord du Centre de Ressources Informatiques.

***

Ressources informatiques de l'INALCO

DECLARATION DE L'ETUDIANT

Je, soussigné :

Nom :
Prénom :
Département :

utilisateur des ressources informatiques de l'INALCO, certifie avoir pris connaissance de la Charte du Bon Usage des ressources informatiques de INALCO, de son annexe et de ses recommandations et m'engage à m'y conformer strictement. (faire précéder la signature de la mention "lu et approuvé")

Paris, le
Signature :