ICP
INSTITUT CATHOLIQUE DE PARIS

Charte d'utilisation des ressources informatiques et réseau de l'ICP

1. Préambule. Le cadre juridique

Toute organisation est responsable des actes de ses salariés et tout acte illégal effectué par un salarié entraîne la responsabilité pénale du salarié.

Concernant la sécurité informatique, plusieurs types de risques peuvent être retenus :

- Les risques touchant à la sécurité du réseau et des applications
- Les risques d'atteinte à la propriété intellectuelle
- Les risques relatifs à la pornographie, la pédophilie, la diffamation et les injures raciales.

Qui dit délits dit sanctions, c'est ainsi que depuis 1978, se met en place un Droit dit Droit de l'Informatique ou encore Droit de la Sécurité des Systèmes Informatiques.

L'ICP, consommatrice d'informatique, utilisatrice des réseaux et productrice, notamment de données scientifiques, n'échappe pas aux risques potentiels et se doit de faire respecter la réglementation en ce domaine.

La présente charte a pour objet de préciser, en accord avec la législation, les responsabilités des utilisateurs des installations informatiques de l'Université afin d'assurer un usage correct des ressources informatiques et des services réseau avec des règles minimales de courtoisie et de respect d'autrui. Elle fait également connaître aux utilisateurs les mesures de sécurité adoptées. En contrepartie de la vigilance demandée à chacun, l'Université s'engage par l'intermédiaire de la Direction des Systèmes d'Informations (DSI) à assurer la qualité attendue en matière d'infrastructures informatiques et réseau en fonction des besoins et dans la mesure de ses moyens.

Cette charte a été approuvée par le Conseil Rectoral.

Les articles 1 à 9 s'appliquent à tous les utilisateurs des ressources informatiques de l'Université. L'article 10 est propre aux administrateurs de sous-réseaux et de serveurs et l'article 11 aux associations étudiantes.

21 rue d'Assas 75270 Paris cedex 06
Tél. 33 (0)1 44 39 52 00 - Fax 33 (0)1 44 45 27 14
Établissement privé d'enseignement supérieur – Association reconnue d'utilité publique

Article 1er - Définitions

Le terme « ressources informatiques » désigne les moyens de traitement de l'information disponibles à l'ICP, en incluant ceux qui offrent une possibilité de connexion à distance.

Le terme « ressource réseau » désigne tous les moyens de communication informatique offerts par l'ICP, incluant notamment tous les services réseaux et Internet (par exemple, Web, messagerie, forums), ainsi que tout équipement de transmission de données.

Le terme « utilisateur » désigne toute personne ayant accès ou utilisant les ressources informatiques ou réseau de l'université.

Le terme « services Internet » désigne tout « service réseau » offert par l'infrastructure de l'ICP, et en particulier, la messagerie électronique, les forums, la messagerie instantanée, les services d'hébergement de pages Web et l'accès distant, applications, etc..

Le terme « ressources documentaires électroniques » désigne tous les catalogues informatisés, périodiques électroniques, bases de données en ligne ou sur cédéroms mis à disposition des utilisateurs par le service commun de documentation de l'Université.

L'expression « membre de la communauté universitaire » de l'ICP désigne tous les enseignants-chercheurs, chercheurs et personnels administratifs et techniques de l'ICP, tous les vacataires et étudiants de l'ICP, tous les chercheurs invités ou associés des centres de recherche de l'ICP et tous les diplômés.

Le terme association autorisée désigne toute association d'étudiants domiciliée et hébergée à l'université et autorisée à bénéficier d'une connexion au réseau de l'université.

Article 2 - Règles d'accès aux ressources

Les ressources de l'ICP sont exclusivement réservées à une utilisation dans le cadre :

- De l'activité professionnelle du personnel de l'université.
- Des activités de recherche, d'étude, d'enseignement, de développement technique, de transfert de technologie, de diffusion d'informations scientifiques, techniques et culturelles, d'expérimentation de nouveaux services présentant un caractère d'innovation technique, mais également toute activité administrative et de gestion accompagnant ces activités.

Les utilisateurs doivent être membres de la communauté universitaire de l'ICP.

Un utilisateur perd son habilitation à utiliser les ressources de l'université dès lors qu'il perd son statut de membre de la communauté universitaire de l'ICP. Des exceptions à cette règle peuvent être accordées par la DSI.

Article 3 - Règles de sécurité

La sécurité des infrastructures informatiques et Internet, nonobstant les dispositifs techniques que l'université installe, est l'affaire de tous les utilisateurs. Ceux-ci doivent donc respecter un certain nombre de règles de base destinées à garantir la sécurité de tous et l'intégrité des infrastructures :

- Les comptes ouverts aux utilisateurs sont rigoureusement personnels
- Ceux-ci doivent être protégés par un mot de passe qui respecte les règles de mise en place des mots de passe (voir annexe A).
- Les utilisateurs ne doivent communiquer leurs mots de passe sous aucun prétexte.
- Il est rigoureusement interdit de mettre en place des services Internet sans autorisation des responsables sécurité.
- Toute tentative d'intrusion constatée par un utilisateur doit être signalée dans les plus brefs délais aux responsables sécurité.
- L'ouverture des fichiers joints aux emails ou enregistrés sur clé USB doit être particulièrement surveillée.
- Toute recommandation du responsable sécurité, concernant notamment la mise à jour de logiciels pouvant présenter des failles de sécurité, doit être suivie dans les plus brefs délais.
- Les utilisateurs ne doivent jamais quitter un poste de travail sans se déconnecter de l'application et du réseau.
- Les utilisateurs s'engagent à ne pas mettre à la disposition d'utilisateurs non autorisés un accès aux systèmes, au réseau ou à des données, à travers des matériels dont ils ont l'usage.
- Tout matériel informatique ne peut être relié au réseau que par un personnel habilité.
- Il est interdit de relier simultanément un matériel informatique au réseau de l'université et à un autre réseau, offrant l'accès à Internet (connexion modem, ADSL, …).
- Il est interdit de mettre en place des programmes destinés à contourner les mesures de sécurité.
- Des fichiers ne peuvent être déposés ou consultés ou modifié sur un serveur que dans des conditions prévues par le responsable du serveur.

Article 4 - Règles de déontologie

L'utilisateur s'engage à ne pas effectuer d'opération qui pourraient conduire à :

- Masquer son identité ou usurper l'identité d'autrui,
- S'approprier le mot de passe d'un autre utilisateur,
- Altérer, modifier ou consulter des données appartenant à d'autres utilisateurs sans autorisation ou sans en avoir la légitimité quand bien même ceux-ci ne les auraient pas protégés. Cette règle s'applique notamment aux boîtes à lettres électroniques,
- Perturber le fonctionnement normal du réseau,
- Utiliser les ressources informatiques et en particulier le réseau de façon intentionnelle dans le but de les saturer ou de les détourner à des fins personnelles,

21 rue d'Assas 75270 Paris cedex 06
Tél. 33 (0)1 44 39 52 00 - Fax 33 (0)1 44 45 27 14
Établissement privé d'enseignement supérieur – Association reconnue d'utilité publique

- Modifier ou détruire des informations présentes sur un système, sans autorisation
- Se connecter sur un site ou un matériel informatique sans y être autorisé.

Par ailleurs, l'utilisateur s'engage à suivre les instructions de la DSI concernant la déclaration à la CNIL de la constitution de tout fichier comportant des données nominatives.

Article 5 -Règles d'utilisation des services Internet et des ressources documentaires électroniques

Conformément aux dispositions légales, les utilisateurs des services Internet s'engagent à ne pas utiliser les ressources de l'université pour tenir des propos (oraux ou écrits) à caractère insultants, diffamatoires, racistes, pédophiles ou attentatoires au respect d'autrui, à ne pas porter atteinte à l'intégrité d'un autre utilisateur ou à sa sensibilité notamment par des messages, textes ou images provocants et à pas émettre d'opinion personnelle étrangère à son activité professionnelle ou susceptible de porter préjudice à l'université. Les utilisateurs sont fermement encouragés à respecter les règles de politesse d'usage sur Internet. Ces règles sont applicables quel que soit le service utilisé, en particulier pour les forums, messagerie électronique et dialogue en direct.

Conformément à la réglementation applicable, l'Université exerce une surveillance des pages Web qu'elle stocke afin d'empêcher la diffusion d'informations faisant l'apologie des crimes de guerre ou des crimes contre l'humanité, incitant à la haine raciale, ou ayant un caractère pédophile, raciste ou pornographique.

L'envoi massif de messages électroniques non désirés (Spam) est totalement prohibé.

La DSI pourra être amenée à supprimer les messages les plus anciens dans le cas où une boîte à lettres électronique atteint une taille maximale. D'une façon générale, des modifications de paramètres pourront être faites par la DSI pour assurer le fonctionnement de la messagerie.

Les utilisateurs s'engagent par ailleurs à respecter les dispositions légales et réglementaires concernant la propriété intellectuelle. Il est notamment interdit de mettre à disposition par l'intermédiaire de l'espace Web offert par l'université des contenus protégés, de reproduire, de diffuser ou de céder les résultats de la consultation d'une base de donnée ou d'un cédérom au bénéfice d'un utilisateur non autorisé, d'exploiter commercialement des données résultant de la consultation d'une base de données ou d'un cédérom, de procéder à des impressions ou téléchargements contraires aux licences d'exploitation, d'incorporer des extraits de produits sous licence dans des supports de cours sans mention de sources ou de copyright, d'incorporer sans permission écrite du concédant des extraits de produits sous licence dans le cadre de programmes d'enseignement à distance.

La consultation de sites pornographiques et pédophiles est interdite.

Article 6 - Dispositifs techniques de protection des infrastructures

L'université se réserve la possibilité de mettre en place, dans le respect de la législation applicable et notamment de la loi sur l'Informatique et les Libertés, des dispositifs de filtrage de contenu destinés à assurer la protection des infrastructures. Ces logiciels peuvent inspecter le

contenu des communications informatisées à la recherche de fichiers ou de programmes qui pourraient mettre en danger l'intégrité des ressources informatiques de l'université.

Des logiciels d'anti-virus et d'anti-spams sont mis en place sur les serveurs de messagerie.

Dans le cas où un virus est détecté, le message n'est pas délivré.

Enfin, dans le cas où un fichier joint serait trop lourd, le message n'est pas délivré / n'est pas envoyé

Article 7 - Utilisation des logiciels

Un utilisateur ne peut installer de logiciels sur son poste sans autorisation du responsable informatique compétent. Il est interdit :

- D'installer des logiciels à caractère ludique.
- D'installer des logiciels dont l'université ne possède pas de licence.
- De faire des copies de logiciels commerciaux.
- De développer des programmes potentiellement dangereux pour les ressources informatiques et réseau sans autorisation expresse des responsables sécurité.
- De dupliquer, donner ou vendre des logiciels ou des documentations mis à disposition par l'Université.
- De contourner les restrictions d'utilisation d'un logiciel.

Parallèlement à cela, la DSI est responsable de la mise à jour des logiciels utilisés par les salariés de l'ICP dans le cadre de leur travail/fonction/poste.

Article 8 - Rappel des lois spécifiques au Droit de l'Informatique et des dispositions du code pénal concernant les infractions en matière informatique

Les lois :

Loi du 6/01/78 sur l'Informatique, les fichiers, les libertés – Elle crée la Commission Nationale Informatique et Libertés et met en place des procédures de contrôle des traitements informatisés des données nominatives. (Plus d'informations http://www.cnil.fr)

Loi du 3/07/85 sur la protection des logiciels – Elle interdit à l'utilisateur d'un logiciel toute reproduction autre que l'établissement d'une copie de sauvegarde.

Loi du 5/01/88 (loi GODFRAIN) relative à la fraude informatique – Elle vise à lutter contre la fraude informatique en réprimant :

- les accès ou le maintien frauduleux dans un système informatique,
- les atteintes accidentelles ou volontaires au fonctionnement,
- la falsification de documents informatisés et leur usage,
- la tentative de ces délits,
- l'association ou l'entente en vue de les commettre.

Les dispositions du code pénal :

Article 323-1 - (Ordonnance nº 2000-916 du 19 septembre 2000 art. 3 Journal Officiel du 22 septembre 2000 en vigueur le 1er janvier 2002)

Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni d'un an d'emprisonnement et de 15000 euros d'amende.

Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de deux ans d'emprisonnement et de 30000 euros d'amende.

Article 323-2 - (Ordonnance nº 2000-916 du 19 septembre 2000 art. 3 Journal Officiel du 22 septembre 2000 en vigueur le 1er janvier 2002)

Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de trois ans d'emprisonnement et de 45000 euros d'amende.

Article 323-3 - (Ordonnance nº 2000-916 du 19 septembre 2000 art. 3 Journal Officiel du 22 septembre 2000 en vigueur le 1er janvier 2002)

Le fait d'introduire frauduleusement des données dans un système de traitement automatisé ou de supprimer ou de modifier frauduleusement les données qu'il contient est puni de trois ans d'emprisonnement et de 45000 euros d'amende.

Article 323-4 - La participation à un groupement formé ou à une entente établie en vue de la préparation, caractérisée par un ou plusieurs faits matériels, d'une ou de plusieurs des infractions prévues par les articles 323-1 à 323-3 est punie des peines prévues pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée.

Article 323-7 - La tentative des délits prévus par les articles 323-1 à 323-3 est punie des mêmes peines.

Article 323-5 - Les personnes physiques coupables des délits prévus au présent chapitre encourent également les peines complémentaires suivantes :

1º L'interdiction, pour une durée de cinq ans au plus, des droits civiques, civils et de famille, suivant les modalités de l'article 131-26 ;

2º L'interdiction, pour une durée de cinq ans au plus, d'exercer une fonction publique ou d'exercer l'activité professionnelle ou sociale dans l'exercice de laquelle ou à l'occasion de laquelle l'infraction a été commise ;

3º La confiscation de la chose qui a servi ou était destinée à commettre l'infraction ou de la chose qui en est le produit, à l'exception des objets susceptibles de restitution ;

4º La fermeture, pour une durée de cinq ans au plus, des établissements ou de l'un ou de plusieurs des établissements de l'entreprise ayant servi à commettre les faits incriminés ;

5º L'exclusion, pour une durée de cinq ans au plus, des marchés publics ;

6º L'interdiction, pour une durée de cinq ans au plus, d'émettre des chèques autres que ceux qui permettent le retrait de fonds par le tireur auprès du tiré ou ceux qui sont certifiés ;

7º L'affichage ou la diffusion de la décision prononcée dans les conditions prévues par l'article 131-35.

Article 9 - Sanctions encourues

L'utilisateur qui enfreint une des règles de la présente charte encourt d'éventuelles sanctions disciplinaires et/ou pénales et/ou la suppression de son accès aux ressources informatiques et réseau de l'université.

Article 10 - Responsabilités des administrateurs systèmes, réseau et bases de données

Les administrateurs systèmes/réseau/Bases de données sont les personnes qui gèrent les sous-réseaux connectés au réseau de l'Université ainsi que les serveurs sur lesquels sont installés les différents services mis à la disposition des utilisateurs (services Internet, applications de gestion, services pédagogiques, services pour la recherche et la documentation).

Les administrateurs ont la charge de la bonne qualité du service fourni aux utilisateurs dans la limite des moyens alloués. Ils ont le droit d'entreprendre toute démarche nécessaire au bon fonctionnement des moyens informatiques de l'Université en accord avec les responsables sécurité.

Les administrateurs ont le devoir d'informer, dans la mesure du possible, les utilisateurs de toute intervention nécessaire, susceptible de perturber ou d'interrompre l'utilisation habituelle des moyens informatiques.

Les administrateurs ont l'obligation de préserver et de respecter la confidentialité des informations privées qu'ils sont amenés à connaître dans le cadre de leur activité.

Article spécifique aux associations étudiantes

Article 11 - Responsabilités des associations étudiantes connectées au réseau de l'Université

Toutes les dispositions et règles précédemment décrites s'appliquent aux associations en tant qu'usagers de l'université.

Les connexions au réseau de l'Université des associations étudiantes qui en font la demande sont effectuées sous la responsabilité du directeur de la DSI.

Les présidents d'associations étudiantes sont tenus de faire respecter l'emploi des matériels de leur association connectés au réseau de l'Université aux termes de la présente charte. Ils ont le devoir de surveiller les traces des connexions (identité des matériels informatiques et des utilisateurs, URLs visités) et de signaler toute anomalie au Responsable Sécurité du Système Informatique sans délai.

Les associations qui se connectent au réseau de l'Université ne doivent pas gêner le bon fonctionnement du réseau. En cas de perturbations sur la bande passante pour les activités principales de l'Université, la DSI se réserve le droit de déconnecter les matériels incriminés.

Toute infraction à la présente charte entraînera la déconnection immédiate des matériels de l'association concernée.

Le président d'association autorisée a la responsabilité de l'application de la présente charte au sein de son association et en particulier de la non divulgation des mots de passe.

ENGAGEMENT PERSONNEL DE L'UTILISATEUR

Je soussigné ……., demeurant à ……., déclare

avoir pris connaissance des dispositions de la présente charte, et m'engage à les respecter.

Fait à Paris., le ……..

Signature :

ENGAGEMENT DU PRESIDENT D'ASSOCIATION (pour les associations autorisées seulement)

Je soussigné ……., Président de l'association……..

reconnaît avoir pris connaissance des dispositions de la présente charte, et m'engage à les

respecter et à les faire respecter par les membres de l'association.

Fait à Paris, le ……..

Le président de l'association

……

(Nom et Prénom)

Annexe A. Règles de création de mots de passe

Les mots de passe doivent :

- Comporter au moins 9 caractères
- Ne pas être un mot présent dans un dictionnaire (quelle que soit la langue)
- Ne pas être une permutation d'un mot présent dans un dictionnaire (quelle que soit la langue)
- Ne pas être une information se rapportant directement au titulaire du compte (date de naissance, nom d'animal de compagnie…)
- Comporter au moins 2 chiffres
- Comporter de préférence 2 caractères spéciaux (non contigus).

icp.fr
21 rue d'Assas 75270 Paris cedex 06
Tél. 33 (0)1 44 39 52 00 - Fax 33 (0)1 44 45 27 14
Établissement privé d'enseignement supérieur – Association reconnue d'utilité publique