

CHARTRE DE L'UTILISATEUR

DES RESSOURCES INFORMATIQUES ET DES SERVICES INTERNET DE L'IPST-CNAM

Préambule

Ce document est un code de bonne conduite précisant la responsabilité des utilisateurs en accord avec la législation afin d'instaurer un usage convenable des ressources informatiques et des services Internet, dans le respect des dispositions légales et réglementaires en vigueur, avec des règles minimum de courtoisie et de respect d'autrui.

Définitions

On désignera le terme « ressources informatiques », les moyens informatiques (matériel ou logiciel) mis à disposition directement ou par accès à distance sur le réseau administré par l'IPST-Cnam.

On désignera par « services Internet » la mise à disposition par des serveurs locaux ou distants des moyens d'information et d'échange : site internet, plate-forme numérique d'enseignement, portail, etc.

On désignera par le terme « utilisateur » la personne ayant accès aux ressources informatiques et services Internet de l'établissement.

Conditions d'accès aux ressources et aux services

L'accès aux ressources informatiques, aux services Internet, aux partages réseaux est autorisé dans les cadres des activités professionnelles, d'enseignement ou de recherche.

Signataire de la charte Renater, nous respectons et faisons appliquer les recommandations de cette dernière (https://www.renater.fr/IMG/pdf/charte_fr.pdf).

L'accès est délivré par le Directeur de l'établissement, grâce à la création d'un compte sur le système d'information dont les données sont strictement personnelles et inaccessibles même temporairement à un tiers.

Ces autorisations peuvent être retirées à tout moment. Elles prennent automatiquement fin avec l'activité qui les a générées : départ professionnel, licenciement, mutation, arrêt des enseignements, etc.

En fonction des besoins ou des impératifs de sécurité informatique, l'établissement pourra prévoir des restrictions spécifiques ou ponctuelles sur ces données.

Règles d'utilisation, de sécurité et de bon usage

Tout utilisateur est responsable de son usage des ressources informatiques et du réseau auquel il a accès. Il a aussi la charge, à son niveau, de contribuer à la sécurité générale et à celle de l'établissement.

L'utilisation de ces ressources doit être rationnelle et bienséante afin d'en éviter la surcharge ou le détournement à des fins personnelles.

En particulier :

- Il doit appliquer les consignes de sécurité de l'établissement,
- Il doit assurer la protection de ses données en utilisant différents moyens de sauvegarde individuelle,
- Il doit signaler toute tentative de violation de son compte et, de façon générale, toute anomalie dès lors qu'il la constate,
- Il choisit des mots de passe sûrs (suite d'au moins huit caractères, avec majuscules, chiffres et/ou caractères de ponctuation). Il sera gardé secret et en aucun cas communiqué à des tiers,
- Il s'engage à ne pas mettre à la disposition d'utilisateur non autorisé un accès aux systèmes ou aux réseaux à travers des matériels dont il a usage,
- Il ne doit pas utiliser ou essayer d'utiliser un compte autre que le sien,
- Il ne doit pas installer de logiciel. Sont disponibles seulement ceux fournis par l'établissement,
- Il ne doit pas tenter de lire, modifier, copier ou détruire des données autres que celles qui lui appartiennent en propre, directement ou indirectement.
- **Il ne doit pas quitter le poste de travail sans se déconnecter en laissant les ressources ou services accessibles.**

Toute violation des présentes obligations sont susceptibles d'engager la responsabilité pénale de son auteur.

Confidentialité

L'accès par les utilisateurs aux informations et aux documents, partagés ou non, sont contrôlés et réservés à ceux qui leurs sont propres.

Il est interdit de prendre connaissance des informations détenues par d'autres utilisateurs quand bien même celles-ci seraient disponibles ou mal protégées.

Respect de la législation

Il est strictement interdit d'effectuer des copies de logiciels ou progiciels quel qu'en soit l'usage. Seule est autorisée la copie de sauvegarde dans les conditions prévues par le Code de la propriété intellectuelle.

Les logiciels installés font l'objet de licence dont les droits d'utilisation sont acquittés par l'établissement.

Préservation de l'intégrité des systèmes informatiques

L'utilisateur est partie prenante de la sécurité informatique. Il s'engage à ne pas perturber le bon fonctionnement des systèmes informatiques et des réseaux, que ce soit par des tentatives d'intrusion ou l'introduction d'un logiciel malveillant tel que : virus, chevaux de Troie, ...

Eventuellement dans un cadre pédagogique ou de recherche, le développement de logiciels malveillants ne pourrait être réalisé qu'avec l'accord du directeur de l'établissement, et cela sous contrôle, en respectant les consignes de sécurité définies à cette occasion.

Le Pôle Système d'Information est garant de la mise en place des outils et logiciels de protection.

Usage des Services Internet (Web, messagerie, forum, réseaux sociaux...)

L'emploi de ces services est strictement réservé aux activités professionnelles, pédagogiques ou de recherche, en respect des directives Renater et des lois en vigueur.

L'utilisateur doit respecter les règles suivantes

Règles de bon usage :

- Il ne doit pas se connecter sur des serveurs autres que ceux autorisés,
- Il ne doit pas nuire au bon fonctionnement des serveurs auxquels il accède,
- Il ne doit pas usurper l'identité, ni intercepter de communication,
- Il ne doit pas rendre disponibles les services proposés à des tiers,
- Il ne doit pas déposer de fichiers, de logiciels sur un serveur sauf s'il dispose des autorisations requises,
- Il doit faire preuve de correction à l'égard de ses interlocuteurs dans les échanges électroniques par courrier, forum de discussion, réseaux sociaux ...
- Il ne doit pas porter préjudice à l'établissement ou à des personnels par des opinions personnelles
- Il doit respecter les lois et celles relatives aux publications à caractère injurieux, raciste, pornographique ou diffamatoire.

Disposition de filtrage de trafic

Une application matérielle spécialisée dans les réseaux filtre le trafic provenant d'Internet.

Son objectif est d'examiner les flux de données, les demandes d'accès aux réseaux publics du site et d'autoriser ou non leurs passages.

Les fichiers de trace sont conservés pendant un an conformément à la législation.

La mise en œuvre de cette solution est faite dans le respect de la législation et doit donner lieu à une information aux représentants du personnel.

Surveillance et contrôle de l'utilisation des ressources

Pour garantir la confidentialité, l'intégrité et la disponibilité des données, les ressources matérielles ou logicielles ainsi que les fichiers de trace peuvent être analysés et contrôlés dans le respect de la législation française et des lois sur l'informatique et liberté.

La mise en œuvre de cette solution est faite dans le respect de la législation et doit donner lieu à une information aux représentants du personnel.

Les principales lois françaises

Il est rappelé que toute personne présente sur le sol français doit respecter la législation française, en particulier celle de la sécurité informatique :

- ❖ La loi du 6 janvier 1978 dite « Informatique et Libertés » (cf. le site web de la CNIL <http://www.cnil.fr>),
- ❖ La législation relative à la fraude informatique (article 323-1 à 323-7 du Code pénal, cf. <http://www.legifrance.gouv.fr>),
- ❖ La législation relative à la propriété intellectuelle (cf. <http://www.legifrance.gouv.fr>),
- ❖ La loi du 4 août 1994 relative à l'emploi de la langue française (cf. <http://www.legifrance.gouv.fr>),
- ❖ La législation applicable en matière de cryptologie (cf. <https://www.ssi.gouv.fr/administration/reglementation/controle-reglementaire-sur-la-cryptographie/>).

Application

La présente charte s'applique à l'ensemble des agents, des enseignants tous statuts confondus, aux contractuels, aux vacataires et à l'ensemble des personnes utilisant les moyens informatiques mis à leur disposition.