Charte Informatique de l'Université de Versailles Saint-Quentin-en-Yvelines

La présente charte a pour objet de définir les règles d'utilisation des moyens informatiques au sein de l'Université de Versailles Saint-Quentin-en-Yvelines, et de rappeler à chacun des utilisateurs ses responsabilités.

1 Champ d'applications de la charte

Les règles et obligations ci-dessous énoncées s'appliquent à toute personne ; en particulier enseignants, chercheurs, enseignants-chercheurs, étudiants, personnels administratifs ou techniques ; autorisée à utiliser les moyens et systèmes informatiques de l'Université de Versailles Saint-Quentin-en-Yvelines.

Ces derniers comprennent notamment les serveurs, stations de travail et micro-ordinateurs et leurs périphériques situés dans les services, les salles de cours ou d'informatique et les laboratoires de l'Université.

Le respect des règles définies par la présente charte s'étend également à l'utilisation des systèmes informatiques d'organismes extérieurs à l'Université, systèmes accessibles par l'intermédiaire des réseaux de l'établissement, par exemple le réseau Internet.

2 Conditions d'accès aux ressources informatiques de l'Université

L'utilisation des moyens informatiques de l'Université a pour objet exclusif de mener des activités de recherche, d'enseignement ou d'administration. Sauf autorisation préalable délivrée par l'Université, ces moyens ne peuvent être employés en vue d'une utilisation ou de la réalisation de projets ne relevant pas des missions de l'Université ou des missions confiées aux utilisateurs.

Chaque utilisateur se voit attribuer des codes d'accès en fonction de ses besoins (accès internet, accès aux applications de gestion, accès à des serveurs particuliers, etc.).

Ces codes d'accès sont strictement personnels et incessibles. Ils sont temporaires et sont retirés si la qualité de l'utilisateur ne le justifie plus.

Chaque utilisateur est responsable de l'utilisation qui en est faite. En particulier :
- il prendra soin de choisir un mot de passe ne correspondant ni à un mot, ni à un nom propre d'aucune langue que ce soit ;
- il ne communiquera pas ce mot de passe à une tierce personne ;
- il préviendra le Centre de Services Informatiques si un code d'accès ne lui permet plus de se connecter, s'il soupçonne que son compte a été usurpé. D'une façon plus générale, il informera le responsable informatique de toute anomalie qu'il pourrait constater.

3 Devoir de l'utilisateur

Chaque utilisateur s'engage à respecter les règles de la déontologie informatique et notamment à ne pas effectuer intentionnellement des opérations qui pourraient avoir pour conséquences :
- de masquer sa véritable identité ;
- d'usurper l'identité d'autrui ;
- de s'approprier le mot de passe d'un autre utilisateur ;
- d'altérer, de modifier des données ou d'accéder à des informations appartenant à d'autres utilisateurs du réseau ou à l'Université, sans leur autorisation ;
- de porter atteinte à l'intégrité d'un autre utilisateur ou à sa sensibilité, notamment par l'intermédiaire de messages, textes ou images provocants ;
- d'interrompre ou de perturber le fonctionnement normal du réseau ou d'un des systèmes connectés au réseau ;
- de modifier ou de détruire des informations sur un des systèmes ;
- d'utiliser ou de développer des programmes mettant sciemment en cause l'intégrité des systèmes informatiques ;
- de se connecter ou d'essayer de se connecter sur un site sans y être autorisé.

Si dans l'accomplissement de son travail ou de ses missions, l'utilisateur est amené à constituer des fichiers, il est rappelé que la loi "informatique et libertés" impose, préalablement à leur constitution, que les fichiers comportant un traitement de données nominatives fassent l'objet d'une déclaration ou d'une demande d'avis auprès de la Commission Nationale Informatique et Libertés (CNIL). Pour plus d'informations, contacter le Centre de Services Informatiques (CSI).

L'utilisateur ne devra en aucun cas :
- installer des logiciels à caractère ludique ;
- faire une copie d'un logiciel commercial ;
- contourner les restrictions d'utilisation d'un logiciel ;
- contrevenir aux lois sur la propriété intellectuelle, littéraire et artistique

Chaque utilisateur s'engage à prendre soin du matériel et des locaux informatiques mis à sa disposition.
Il informe le CSI de toute anomalie constatée.

4 Information des utilisateurs sur la gestion des systèmes et réseaux informatiques

4.1 Responsabilités des administrateurs systèmes/réseau/SGBD

Les administrateurs systèmes/réseau/SGBD sont les personnes qui gèrent les machines connectées 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.

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 le devoir d'informer immédiatement le responsable sécurité de l'université (ou son suppléant) de toute tentative d'intrusion sur un système, ou de tout comportement délictueux d'un utilisateur.

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

4.2 Fichiers de traces

Les services utilisés génèrent, à l'occasion de leur emploi, "des fichiers de traces".
Ces fichiers sont essentiels à l'administration des systèmes. Ils servent en effet à remédier aux dysfonctionnements des services ou systèmes informatiques utilisés. Ces fichiers conservent des informations par exemple concernant la messagerie (expéditeur, destinataire(s), date), mais aussi heures de connexion aux applications de gestion, au service de connexion à distance, numéro de la machine depuis laquelle les services sont utilisés, etc...
Ce type de traces existe pour l'ensemble des services Internet. Ces fichiers ne sont utilisés que pour un usage technique. Toutefois, dans le cadre d'une procédure judiciaire ces fichiers peuvent être mis à la disposition de la justice.

5 Sanctions

L'utilisateur qui contreviendrait aux règles précédemment définies s'expose au retrait de son compte informatique, ainsi qu'aux poursuites disciplinaires et pénales, prévues par les textes législatifs et réglementaires en vigueur (Articles 323-1 à 323-7 du code pénal).

Approuvée le 11 Juin 2002 par le Conseil d'Administration de l'Université de Versailles Saint-Quentin-en-Yvelines