Charte du bon usage des moyens informatiques de l'Université de Poitiers

1. Objet

La présente charte, approuvée par le CA de janvier 2007, a pour objet de définir les conditions d'utilisation et les règles de bon usage des moyens informatiques de l'Université de Poitiers et d'assurer le développement de l'utilisation de l'informatique dans le respect des lois et règlements.

2. Domaine d'application

La charte s'applique à l'ensemble des personnes qui, quel que soit leur statut, ont accès aux moyens informatiques de l'Université de Poitiers.

3. Moyens informatiques

Sont **notamment** constitutifs de moyens informatiques, les serveurs, stations de travail, postes de consultation, les réseaux internes et externes de l'Université de Poitiers, les micro-ordinateurs des services, laboratoires, instituts, centres, facultés, ainsi que l'ensemble du parc logiciel, des bases de données, des produits multimédias ou des périphériques affectés au fonctionnement des éléments décrits.

Sont également considérés comme moyens informatiques, les ressources extérieures accessibles par l'intermédiaire des réseaux de l'Université de Poitiers et notamment le réseau RENATER.

4. Utilisations

4.1 Finalité de l'utilisation des moyens informatiques de l'Université de Poitiers

L'utilisation des moyens informatiques est limitée au strict cadre et aux seuls besoins de l'activité et de la vie universitaire.

4.2 Autorisations particulières

Toute autre utilisation des moyens informatiques de l'Université de Poitiers doit être préalablement autorisée par le Président de l'Université ou son représentant.

4.3 Utilisations prohibées

Sont strictement prohibées les utilisations contraires aux lois et règlements en vigueur et notamment celles qui ont pour objet ou pour effet, la diffusion d'idéologies politiques, ou qui sont de nature à porter atteinte aux bonnes mœurs, à la dignité, à l'honneur, ou à la vie privée des personnes.

4.4 *Utilisations* par les organisations syndicales

Les listes de diffusion syndicales ainsi que les pages syndicales ouvertes sur le site intranet de l'université sont libres d'expression. Des restrictions ne peuvent intervenir que conformément à la législation en vigueur.

5. Utilisateurs

5.1 Identification des utilisateurs

Par utilisateur, on entend toute personne qui, à titre habituel ou non, professionnel ou non, est autorisée à accéder aux moyens informatiques de l'Université de Poitiers.

5.2 Obligations des utilisateurs

5.2.1 Règles générales

Les utilisateurs sont tenus de respecter la charte des bons usages de l'informatique de l'Université de Poitiers.

Les utilisateurs doivent respecter les lois et règlements en vigueur ainsi que les règles de courtoisie et de politesse lors de l'utilisation des moyens informatiques de l'Université de Poitiers.

Les utilisateurs doivent faire une utilisation non-abusive des moyens informatiques auxquels ils ont accès.

Les utilisateurs doivent respecter les mesures de sécurité des moyens informatiques prévues à l'article 8 de la présente charte.
Les utilisateurs sont tenus de se conformer aux décisions des responsables informatiques.

5.2.2 Fichiers des utilisateurs

Les utilisateurs peuvent créer des fichiers privés pour lesquels ils ont le droit d'accès exclusif.
Ces fichiers doivent être considérés comme privés tant que leur créateur ne les a pas mis à la disposition du public.
Sont interdites la destruction, l'altération ou la reproduction d'un fichier mis à la disposition du public, en dehors des cas où elles sont expressément autorisées.

5.2.3 Préservation des matériels et locaux

Les utilisateurs sont tenus de respecter les matériels, logiciels et locaux mis à leur disposition.
Les utilisateurs qui constatent une dégradation ou un dysfonctionnement doivent, dans les plus brefs délais, informer le responsable informatique.

5.2.4 Pénétration non autorisée dans les moyens informatiques

La pénétration non autorisée et le maintien dans un moyen informatique par un utilisateur sont interdits.
Les utilisateurs ne doivent pas utiliser ou tenter d'utiliser le compte d'un tiers. Est également interdite toute manœuvre qui viserait à accéder aux moyens informatiques sous une fausse identité ou en masquant l'identité véritable de l'utilisateur.

5.2.5 Utilisation des comptes et des dispositifs de contrôle d'accès

Les utilisateurs doivent prendre toutes mesures pour limiter les accès frauduleux aux moyens informatiques, à ce titre ils doivent **notamment** :

- veiller à la confidentialité des codes, mots de passe, cartes magnétiques, clefs ou tout autre dispositif de contrôle d'accès qui leur sont confiés à titre strictement personnel ;
- veiller à la confidentialité des comptes utilisateurs qui leur sont attribués à titre strictement personnel ;
- ne pas prêter, vendre ou céder les comptes utilisateurs, codes et autres dispositifs de contrôle d'accès ou en faire bénéficier un tiers ;
- se déconnecter immédiatement après la fin de leur période de travail sur le réseau ou lorsqu'ils s'absentent ;
- informer immédiatement le responsable informatique et le Responsable de la Sécurité des Systèmes d'Information (RSSI) de toute tentative d'accès frauduleux ou de tout dysfonctionnement suspect ;
- changer régulièrement les codes d'accès ;
- s'assurer que les fichiers qu'ils jugent confidentiels ne soient pas accessibles à des tiers ;
- informer le responsable informatique et le Responsable de la Sécurité des Systèmes d'Information (RSSI) des périodes durant lesquelles ils n'utiliseront pas leurs comptes.

5.3 Responsabilité des utilisateurs

5.3.1 Responsabilité des utilisations

Les utilisateurs sont responsables de l'utilisation qu'ils font des moyens informatiques de l'Université de Poitiers ainsi que de l'ensemble des informations qu'ils mettent à la disposition du public.

5.3.2 Responsabilité des comptes et dispositifs de contrôle d'accès

Les titulaires de comptes, ou d'un dispositif de contrôle d'accès, sont responsables des opérations locales ou distantes effectuées depuis leurs comptes ou sous le couvert des dispositifs de contrôle d'accès qui leur ont été attribués.

5.4 Sanctions

En cas de non respect de leurs obligations, les utilisateurs peuvent se voir appliquer les sanctions prévues à l'article 9.

6. Responsables informatiques

6.1 Nomination

Les directeurs de services, laboratoires, instituts, centres, facultés nomment pour chaque site informatique placé sous leur autorité, un ou plusieurs responsables ci-après désignés responsables informatiques.

6.2 Fonction des responsables informatiques

Les responsables informatiques :

- autorisent les accès aux moyens informatiques ;
- attribuent les comptes et les mots de passe, cartes magnétiques, clefs ou tout autre dispositif permettant de limiter l'accès aux moyens informatiques conformément aux instructions du directeur ;
- définissent les utilisations conformes à la vocation des moyens informatiques mis à la disposition des utilisateurs, sous le contrôle de l'équipe pédagogique ou du directeur ;
- informent les utilisateurs des bons usages tels qu'ils sont définis dans la présente charte ;
- assurent le fonctionnement et la disponibilité normale des moyens informatiques.

6.3 Pouvoir des responsables informatiques

Les responsables informatiques peuvent surveiller les utilisations qui sont faites des moyens informatiques dont ils ont la charge.

Dans le cadre de leurs fonctions, les responsables informatiques peuvent prendre connaissance des fichiers, des données et des travaux des utilisateurs ainsi que des ressources extérieures qu'ils utilisent.

Les responsables informatiques peuvent, en cas d'urgence, prendre toutes les mesures nécessaires pour assurer ou préserver le bon fonctionnement et la disponibilité normale des moyens informatiques qui leur sont confiés.

6.4 Obligations des responsables informatiques

6.4.1 *Confidentialité*

Les responsables informatiques doivent préserver la confidentialité des informations et des fichiers auxquels ils ont accès dans le cadre de leurs fonctions.

6.4.2 *Qualité du service*

Les responsables informatiques doivent s'efforcer de limiter la gêne occasionnée aux utilisateurs par leurs interventions sur les moyens informatiques de l'Université de Poitiers.

Les responsables informatiques doivent s'efforcer d'assurer une disponibilité normale et le bon fonctionnement des moyens informatiques.

6.4.3 *Information*

Les responsables informatiques sont tenus d'informer le Responsable de la Sécurité des Systèmes d'Information (RSSI) et le directeur du Service Commun Informatique et Multimédia *i*-médias de toute violation ou tentative de violation d'accès ou de tout autre élément de nature à mettre en péril la sécurité des moyens informatiques de l'Université de Poitiers.

6.4.4 *Sécurité*

Les responsables informatiques doivent s'assurer que les codes d'accès choisis par les utilisateurs répondent aux exigences de sécurité telles qu'elles sont édictées par le Service Commun Informatique et Multimédia *i*-médias et le Responsable de la Sécurité des Systèmes d'Information (RSSI).

7. Données nominatives

Les traitements automatisés de données nominatives mis en œuvre par l'Université, ses composantes ou par tout utilisateur doivent respecter les dispositions de la loi 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

8. Modification et altération des moyens informatiques

8.1 *Modification des environnements*

En dehors des modifications ne portant pas atteinte au bon fonctionnement des moyens informatiques, aucune modification des environnements logiciels, matériels et périphériques ne pourra être effectuée sans l'accord préalable du responsable informatique.

Par modification d'environnement, on entend toute suppression ou ajout de composants logiciels ou matériels ou tout paramétrage pouvant affecter le fonctionnement normal des moyens informatiques.

8.2 *Virus, chevaux de Troie, bombes logiques*

L'introduction, l'utilisation, la diffusion de tout dispositif logiciel ou matériel qui pourrait altérer les fonctionnalités des moyens informatiques sont interdites.

Les recherches portant sur les virus, chevaux de Troie, bombes logiques et autres dispositifs qui pourraient altérer les fonctionnalités des moyens informatiques doivent être préalablement autorisées par le responsable informatique.

9. Conséquences des manquements à la charte et poursuites

9.1 *Mesures et sanctions applicables par les responsables informatiques*

9.1.1 *Mesures d'urgence*

Les responsables informatiques peuvent en cas d'urgence :

- déconnecter un utilisateur, avec ou sans préavis selon la gravité de la situation ;
- isoler ou neutraliser provisoirement toute donnée ou fichier manifestement en contradiction avec la charte ou qui mettrait en péril la sécurité des moyens informatiques.

9.1.2 *Mesures donnant lieu à information*

Sous réserve que soit informé le directeur ou le responsable du service, les responsables informatiques peuvent :

- avertir un utilisateur ;
- limiter provisoirement les accès d'un utilisateur ;
- à titre provisoire, retirer les codes d'accès et fermer les comptes ;
- effacer, comprimer ou isoler toute donnée ou fichier manifestement en contradiction avec la charte ou qui mettrait en péril la sécurité des moyens informatiques ;
- informer le Responsable de la Sécurité des Systèmes d'Information (RSSI) ;
- informer le Président de l'Université.

9.1.3 *Mesures soumises à autorisation du directeur ou responsable du service*

Sous condition d'autorisation préalable du directeur ou du responsable de service, les responsables informatiques peuvent :

- retirer les codes d'accès ou autres dispositifs de contrôle d'accès et fermer les comptes ;
- interdire à titre définitif à un utilisateur tout accès aux moyens informatiques dont il est responsable.

9.2 *Autres sanctions internes*

Sans préjudice du pouvoir de sanction des centres, instituts, UFR et autres composantes de l'Université de Poitiers, le Président de l'Université peut prendre toutes les sanctions internes qui permettraient d'assurer le respect de la charte et le bon fonctionnement de l'université ou de ses services.

En particulier, des sanctions disciplinaires peuvent être prises, dans le cadre du décret n° 92-657 du 13 juillet 1992 relatif à la procédure disciplinaire dans les établissements publics d'enseignement supérieur.

Les sanctions internes ou disciplinaires ne sont pas exclusives de poursuites civiles ou pénales.

9.3 *Poursuites civiles et pénales*

Le Président peut, après avis du Conseil d'Administration de l'Université, engager des poursuites civiles à l'encontre des utilisateurs.

Le Président peut, après avis du Conseil d'Administration de l'Université, informer le Procureur de la République des infractions commises par les utilisateurs.