



**UNIVERSITE DE REIMS
CHAMPAGNE-ARDENNE**

Charte du bon usage des moyens informatiques

1. Objet

La présente charte a pour objet de définir les conditions d'utilisation et les règles de bon usage des moyens informatiques de l'Université de Reims Champagne-Ardenne 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, quelque soit leur statut, ont accès aux moyens informatiques de l'Université de Reims Champagne-Ardenne.

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 Reims Champagne-Ardenne, les micro-ordinateurs des services, laboratoires, instituts, centres de recherche, UFR, 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 Reims Champagne-Ardenne et notamment le réseau RENATER.

4. Utilisations

4.1. Finalité de l'utilisation des moyens informatiques de l'Université de Reims Champagne-Ardenne.

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 Reims Champagne-Ardenne 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, raciales ou religieuses, ou qui sont de nature à porter atteinte à l'ordre public, aux bonnes mœurs, à la dignité, à l'honneur, ou à la vie privée des personnes.

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 Reims Champagne-Ardenne.

5.2. Obligations des utilisateurs.

Règles générales

Les utilisateurs sont tenus de respecter la charte de bon usage de l'informatique de l'Université de Reims Champagne-Ardenne.

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 Reims Champagne-Ardenne.

Les utilisateurs doivent avoir 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 (Le Centre de Ressources Informatique ou ses correspondants techniques dans les composantes)

Les utilisateurs sont tenus de s'assurer que l'ordinateur auquel ils ont accès est équipé d'un antivirus à jour.

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 ou leur correspondant.

Pénétration non autorisée dans les moyens informatiques.

La pénétration non autorisée dans un moyen informatique par un utilisateur est interdite.

Les utilisateurs ne doivent pas utiliser ou tenter d'utiliser le compte d'un tiers. Est également interdite toute manoeuvre qui viserait à accéder aux moyens informatiques sous une fausse identité ou en masquant l'identité véritable de l'utilisateur.

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

Les utilisateurs doivent prendre toutes mesures pour limiter les accès frauduleux aux moyens informatiques, et 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.
- s'assurer que les fichiers qu'ils jugent confidentiels ne soient pas accessibles à des tiers.
- informer le responsable informatique ou le correspondant de la fin de validité des moyens mis à leur disposition lors de leur départ définitif de l'université.

Raccordement de matériels aux réseaux de l'université

Aucun matériel actif ne pourra être raccordé aux réseaux de l'université sans l'accord du Centre de Ressources Informatiques ou de ses correspondants techniques dans les composantes.

5.3. Responsabilité des utilisateurs.

Responsabilité des utilisations faites des moyens

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

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.

Listes de diffusion

Tout utilisateur ayant accès à une ou plusieurs listes de diffusion, mises en place par le service de la Communication de l'Université, devra s'engager à ne pas saturer le système de courrier électronique par une utilisation abusive de ces moyens.

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. Le Centre de Ressources Informatiques et les correspondants informatiques

6.1. Nomination des correspondants informatiques

Les Directeurs des composantes proposent au Président de l'Université et au Directeur du Centre de Ressources Informatiques, pour chacun des sites informatiques placés sous leur autorité, un ou plusieurs agents ci-après désignés « correspondants informatiques ».

6.2. Fonction des correspondants informatiques

Les correspondants 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 de composante ;
- 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. Pouvoirs du Centre de Ressources Informatiques et de ses correspondants informatiques

Le personnel Centre de Ressources Informatiques et les correspondants informatiques peuvent surveiller les utilisations qui sont faites des moyens informatiques dont ils ont la charge.

Fichiers de traces

L'ensemble des services utilisés génère, 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 et après accord du Président ces fichiers peuvent être mis à la disposition ou transmis à la justice.

Ces fichiers de trace sont conservés par le Centre de Ressources informatiques dans les conditions réglementaires spécifiées par la CNIL.

6.4. Obligations du Centre de Ressources Informatiques et de ses correspondants informatiques

Confidentialité

Le personnel du Centre de Ressources Informatiques et les correspondants informatiques doivent préserver la confidentialité des informations et des fichiers auxquels ils ont accès dans le cadre de leurs fonctions.

Qualité du service

Ils doivent s'efforcer de limiter la gêne occasionnée aux utilisateurs par leurs interventions sur les moyens informatiques de l'Université de Reims Champagne-Ardenne.

Information

Ils sont tenus d'informer le Responsable Sécurité des Systèmes d'Information (RSSI) ou le directeur du Centre de Ressources Informatiques de l'Université de Reims Champagne-Ardenne 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 Reims Champagne-Ardenne.

Sécurité

Ils doivent s'assurer que les codes d'accès choisis par les utilisateurs répondent aux exigences de sécurité telles qu'elles sont édictées par le Centre de Ressources Informatiques de l'Université de Reims Champagne-Ardenne et le Responsable Sécurité des Systèmes d'Information (RSSI).

7. Données nominatives

Les traitements automatisés de données nominatives mis en oeuvre 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 (CNIL).

8. Modification et altération des moyens informatiques.

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.

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

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,

Mesures donnant lieu à information

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

- limiter provisoirement les accès d'un utilisateur,
- à titre provisoire, retirer les codes d'accès ou autres dispositifs de contrôle 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

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 de la section disciplinaire du Conseil d'Administration de l'Université, le Président de l'Université peut prendre toutes 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.

9.4. Dispositions particulières pour les utilisateurs étudiants

Gestion des boîtes aux lettres des étudiants

Tous les étudiants de Reims Champagne-Ardenne disposent d'une boîte aux lettres personnelle. La taille de celle-ci est limitée. Pour éviter des dysfonctionnements du service de messagerie, le Centre de Ressources Informatiques ou les scolarités pourront être amenés, à la demande expresse de l'étudiant concerné, à supprimer les messages les plus anciens dans le cas où les boîtes aux lettres ont atteint leur taille maximale et de ce fait ne peuvent plus recevoir de nouveaux courriers. D'une façon plus générale, des modifications des paramètres de messagerie pourront être faites pour en assurer le bon fonctionnement

Cette Charte de Bon Usage a été validée par le Conseil d'Administration de l'Université de Reims Champagne-Ardenne en date du 05 juillet 2004.

Le Président de l'Université
de Reims Champagne-Ardenne