



Charte du bon usage de l'informatique et du réseau de l'Université Paul-Valéry

La présente charte a pour objet de définir les règles d'utilisation des moyens informatiques au sein de l'université Paul-Valéry et en particulier, de préciser les droits et devoirs de chacun. Elle représente un engagement mutuel entre l'utilisateur et la communauté universitaire conformément à la législation en vigueur.

La Direction des Systèmes d'Information et du Numérique (DSIN) de l'université Paul-Valéry a pour missions de fournir les moyens informatiques nécessaires à la communauté universitaire et de maintenir le réseau et tous les équipements dans des conditions de fonctionnement et de sécurité optimales.

Le réseau informatique de notre université est relié par l'intermédiaire du Réseau RENATER (Réseau National de télécommunications pour la Technologie, l'Enseignement et la Recherche) à l'internet.

Les ressources informatiques et les services Internet de l'université Paul-Valéry sont mis à la disposition des utilisateurs à des fins d'enseignement, de culture, de recherche et de diffusion d'informations scientifiques, pédagogiques et administratives. Tout utilisateur se doit de respecter les règles de sécurité et de bonne conduite. L'imprudence, la négligence ou la malveillance d'un utilisateur peut avoir des conséquences graves sur le fonctionnement du réseau.

Cette charte a été adoptée par le conseil d'administration de l'université Paul-Valéry le 25 Janvier 2005. Elle est révisable chaque année pour tenir compte de l'évolution des ressources informatiques. Chaque utilisateur est tenu de respecter les règles d'accès instaurées par l'université, qu'elles soient portées à sa connaissance par voie d'affichage ou par messages informatiques.

.....

1) Champ d'application de la charte

Du point de vue informatique, la communauté universitaire est composée de différentes catégories d'utilisateurs tels que :

- Les utilisateurs : étudiants, enseignants, chercheurs, personnels administratifs, techniques et de bibliothèque qui utilisent les systèmes et moyens informatiques mis à leur disposition par l'université Paul-Valéry.
- Les administrateurs systèmes et/ou réseau, responsables techniquement du bon fonctionnement des outils informatiques.
- Les responsables fonctionnels : les directeurs d'UFR, les responsables administratifs, les directeurs de laboratoire ou de service, les enseignants encadrant des étudiants dans le cadre d'activités faisant appel à des ressources informatiques.

Les règles et obligations définies par cette charte s'appliquent à tout utilisateur des moyens informatiques de l'université qu'il soit situé sur le campus principal Route de Mende, sur les sites délocalisés ou bien connecté au réseau depuis son domicile via le serveur d'accès distants de l'université ou par un fournisseur d'accès quelconque.

2) Conditions d'accès aux moyens informatiques

A. Engagements des utilisateurs

a) Identification

Chaque utilisateur se voit attribuer des codes d'accès en fonction de ses besoins (applications de gestion, messagerie, session réseau Windows, accès distant,...).

Les moyens d'accès distribués (carte, clef magnétique, mot de passe...) sont incessibles : ils ne peuvent être ni prêtés, ni donnés, ni vendus. Ils sont temporaires et seront retirés si la fonction de l'utilisateur ne le justifie plus.

Chaque utilisateur est responsable des opérations informatiques, locales ou distantes, faites à partir des ressources qui lui sont allouées. Il doit donc prendre les précautions suivantes :

- garder secret ses mots de passe
- ne pas faciliter l'accès au contenu de son ordinateur (partage de fichiers)
- ne jamais quitter son poste de travail sans en protéger l'accès (verrouillage d'écran)
- informer les responsables sécurité des tentatives de violation de son compte et, de façon générale, de toute anomalie qu'il peut constater.

Les utilisateurs qui travaillent sur des ordinateurs en libre accès (bureaux d'enseignants, salles de cours, halls internet, bibliothèques...) ne réclamant pas d'identification particulière, doivent également respecter les termes de cette charte.

b) Protection des utilisateurs

Les utilisateurs s'engagent :

- à ne pas lire, ni copier, ni modifier, ni détruire un fichier sans l'autorisation de son créateur. La possibilité de lire un fichier n'autorise pas pour autant sa lecture.
- Ne pas intercepter le contenu des communications privées entre utilisateurs. Toutefois, les enseignants ou les administrateurs peuvent être amenés à avoir accès aux comptes des étudiants pour des raisons pédagogiques.
- Ne pas interdire ou limiter l'accès aux ressources informatiques communes de l'université à un autre utilisateur.
- Ne pas autoriser l'accès des ressources à d'autres utilisateurs ou à des personnes extérieures à l'université y compris via les accès distants.
- Ne pas usurper l'identité d'autrui en vue d'accéder à des ressources informatiques.

c) Protection des ressources matérielles

Certaines ressources (serveurs, imprimantes, poste en libre service...) accessibles par le réseau sont privées même si leur accès n'est pas soumis à une identification. Toute utilisation de ces ressources nécessite donc une autorisation sous peine de sanctions prévues en section 4.

Le matériel en libre-service doit faire l'objet d'un soin attentif de la part de chaque utilisateur. Le personnel d'exploitation doit être informé des problèmes rencontrés afin qu'ils soient corrigés dans les délais les plus brefs.

d) L'utilisation des ressources communes

Les ressources informatiques de l'université ne peuvent pas être utilisées à des fins commerciales ou personnelles autres que dans le cadre d'activités de formation, de culture ou de recherche ou à des fins ludiques (jeux multimédia « en réseau » ou autres).

La connexion d'ordinateurs, portables ou non ou encore de périphériques externes tels que les modems est soumise à une déclaration préalable auprès de la Direction des Systèmes d'Information et du Numérique ou de son représentant.

Tout projet d'installation de serveurs doit être étudié avec les administrateurs de la DSIN afin qu'il puisse s'insérer au mieux dans la politique sécurité de l'université.

Les utilisateurs ne doivent pas effectuer d'expérimentation sur la sécurité des systèmes informatiques et réseaux ni sur les virus informatiques sans autorisation préalable. Le développement, l'installation ou la simple détention d'un programme cherchant à contourner la sécurité d'un système ou les protections des logiciels sont interdits. L'installation de logiciels ou utilitaires pouvant porter atteinte au fonctionnement des machines est proscrit.

L'utilisation de tout logiciel participant aux missions de l'université, susceptible de saturer ou de charger le réseau doit faire l'objet d'une concertation préalable avec la DSIN.

e) Aspects légaux

Le piratage informatique est une infraction aux lois régissant les droits de la propriété intellectuelle, droit d'auteur, et la protection juridique des programmes. L'utilisation illégale de logiciels peut entraîner des poursuites judiciaires de la part des auteurs. Sont considérés comme actes de piratage :

- la copie de logiciels sans contrat de licence ou accord de l'éditeur hormis une copie de sauvegarde dans les conditions prévues par le code de la propriété industrielle,
- l'utilisation de logiciels non accompagnés d'un contrat de licence,
- l'utilisation de logiciel sans licence appropriée ou sur plus de postes que prévu par la licence
- les copies ou contrefaçons de CD-ROMs et leur distribution gratuite ou en échange d'argent
- les téléchargements sur internet de musique ou copie de films protégés par des droits d'auteur
- l'usage non conforme aux clauses du contrat,
- le prêt ou la location de logiciels sans l'accord de l'éditeur.

Les utilisateurs doivent respecter les dispositions légales en matière de traitement automatisé de données à caractère personnel, conformément à la loi n°78-17 du 6 janvier 1978 modifiée dite loi « informatique et Libertés ».

Les données à caractère personnel sont des informations qui permettent, sous quelque forme que ce soit, directement ou indirectement, l'identification des personnes physiques auxquelles elles se rattachent. Toutes les créations de fichiers comprenant ce type d'informations et demandes de traitement qui s'y rattachent, y compris lorsqu'elles résultent de croisement ou d'interconnexion de fichiers préexistants, sont soumises aux formalités préalables prévues par la loi « informatique et Libertés ».

En conséquence, tout utilisateur ayant un projet de création d'un tel traitement devra en informer le correspondant informatique et libertés de l'établissement (CIL), préalablement à toute manipulation de données.

Par ailleurs, conformément aux dispositions de cette loi, chaque utilisateur dispose d'un droit d'accès et de rectification relatif à l'ensemble des données le concernant. Ce droit s'exerce en général auprès du responsable du service qui gère le traitement des données dont il s'agit.

Les informations diffusées par le biais des réseaux ne doivent pas :

- porter atteinte à la vie privée ou à l'image d'autrui
- contrevenir aux lois sur la propriété intellectuelle, littéraire et artistique
- faire l'apologie du racisme, de l'antisémitisme et de la xénophobie.

B. Engagements (et missions) des administrateurs

Les ressources informatiques de l'université sont sous la responsabilité des administrateurs système qui ont en charge la bonne qualité du service fourni aux utilisateurs dans la limite des moyens alloués, ils ont pour mission quotidienne le bon fonctionnement du réseau.

Ils s'engagent :

- à prendre toute disposition utile pour permettre le bon fonctionnement des ressources informatiques communes,
- à respecter la confidentialité des fichiers, des courriers, des sorties imprimantes et des journaux auxquels il pourrait avoir accès, ceci dans le cadre du devoir de réserve dû à tout agent de la fonction publique,
- à informer les utilisateurs des interruptions volontaires de service. Ils s'engagent à les minimiser et à choisir les périodes les moins pénalisantes pour les utilisateurs,
- à mettre en œuvre les ressources techniques et humaines requises pour assurer un niveau permanent de sécurité conforme à l'état de l'art et aux règles en vigueur dans ce domaine et pour prévenir les agressions éventuelles à partir ou par l'intermédiaire de son/ses sites.

En cas de dysfonctionnement et afin que cela n'entrave pas le travail de l'ensemble des utilisateurs, les administrateurs peuvent :

- surveiller en détail les sessions de travail d'un utilisateur dans le cas d'utilisation anormale du réseau,
- prendre, avec ou sans préavis, les dispositions nécessaires à l'encontre d'un utilisateur si celui-ci gêne le bon fonctionnement des ressources informatiques,

- effacer ou compresser les fichiers excessifs ou sans lien direct avec une utilisation normale du système informatique,
- mettre fin à des sessions de travail restées trop longtemps inactives ou même interdire l'accès au réseau momentanément.

Actions entreprises pour combattre les virus

Des outils sont mis en place sur les postes des utilisateurs contre les virus. Le paramétrage adopte la stratégie suivante : le logiciel tente de réparer le fichier infecté si la tentative échoue, le fichier est détruit.

Un logiciel d'anti-virus est également mis en place sur le serveur de messagerie évitant ainsi de recevoir des virus et aussi d'en émettre à l'extérieur de l'université. Le destinataire et l'expéditeur sont informés lorsque le message contient un virus, ce message est délivré mais il est épuré du virus. Ce logiciel filtre également les courriers à caractère publicitaire non sollicités (spams) pouvant saturer les messageries des utilisateurs.

3) Recours de l'utilisateur

Le Président de l'université a désigné deux Responsables de la Sécurité des Systèmes d'Information (R.S.S.I) chargés de la sécurité en matière d'informatique et de réseaux pour son établissement.

Les deux RSSIs pourront vous donner ou rechercher toutes les informations nécessaires en cas d'incident car ils sont en relation directe avec la cellule de sécurité du réseau RENATER (CERT-Renater). Ils analyseront l'incident signalé et prendront les mesures adéquates. Ils ont pour mission d'informer le CERT-Renater de toute tentative de piratage et traiter les incidents survenus. Les RSSIs rapportent directement au responsable d'établissement les actes frauduleux réalisés sur son/ses sites par ou à l'encontre de ses utilisateurs. Ils sont les coordonnateurs entre les différents intervenants en cas de problème (hiérarchie, CERT, sites concernés, police).

Les utilisateurs qui subissent un préjudice ou ont remarqué des actions anormales doivent contacter rapidement ces deux personnes. La DSIN pourra vous communiquer leurs coordonnées.

4) Sanctions applicables

Tout utilisateur n'ayant pas respecté la loi peut être poursuivi pénalement. Seul le président d'université peut décider d'engager des poursuites pénales et d'informer à cette fin le Procureur de la République. Les sanctions pénales ne sont pas exclusives de sanctions administratives.

Les utilisateurs ne respectant pas les règles et obligations définies dans cette Charte sont passibles de sanctions internes à l'établissement prévues par les textes du règlement intérieur.

Rappel des principales lois françaises

- **La loi n°78-17 du 6 janvier 1978** modifiée relative à l'informatique, aux fichiers et aux libertés sanctionnée notamment par les articles 226-16 à 226-24 du cde pénal.
- **Le code de la propriété** intellectuelle qui prévoit notamment que les logiciels font partie des œuvres protégées au titre du droit d'auteur.

(cf. notamment article L335-3 du code de la propriété intellectuelle qui qualifie de délit de contrefaçon la violation des droits de l'auteur des logiciels.

- **Les articles 323-1 et suivants du code pénal** qui définissent les délits d'atteintes aux systèmes automatisés de données

Extraits :

« Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de 2 ans d'emprisonnement et de 3000 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 3 ans d'emprisonnement et de 4500 euros d'amende.

Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de 5 ans d'emprisonnement et de 7500 euros d'amende.

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 5 ans d'emprisonnement et de 75000 euros d'amende ».

ENGAGEMENT DE L'UTILISATEUR

Article 1 : A qui s'applique la charte

Tout utilisateur, étudiant, enseignant, chercheur, personnel administratif ou technique, administrateur de systèmes et responsable fonctionnel est soumis à la charte du bon usage de l'informatique et du réseau de l'Université Paul-Valéry.

Article 2 : Utilisation exclusive

Tout utilisateur s'engage à utiliser les moyens informatiques et réseaux mis à sa disposition dans le cadre exclusif de son activité à l'Université Paul-Valéry.

Article 3 : Propriété du binôme mot de passe/espace de travail

Tout utilisateur s'engage à ne pas communiquer son mot de passe et à ne pas prêter son compte à un tiers.

Article 4 : Responsabilité de l'utilisateur

Tout utilisateur est responsable de la pérennité de ses fichiers et de l'intégrité de son espace de travail. Lui seul a la charge de protéger ses fichiers.

Article 5 : Engagement de non-duplication

Tout utilisateur s'engage à ne procéder à d'autres copies de logiciels que celles permettant la sauvegarde de ses propres données. Les logiciels utilisés doivent posséder une licence.

Article 6 : Engagement de vigilance

Tout utilisateur s'engage à signaler toute tentative de violation de son compte en cas de doute.

Article 7 : Responsabilité de la Direction des Systèmes d'Information et du Numérique (DSIN)

Les personnels de la DSIN s'engagent à mettre en œuvre les sécurités réseaux dont ils ont connaissance, à respecter la confidentialité des données.

Article 8 : Sanctions

Tout contrevenant se verra sanctionner au niveau universitaire, conformément aux sanctions prévues par le règlement intérieur de l'établissement, le Président de l'Université Paul-Valéry pourra, si nécessaire, engager des poursuites au niveau pénal.

Article 9 : Durée de vie de l'habilitation à utiliser un compte

Tout utilisateur s'engage à avertir la DSIN s'il doit quitter de façon permanente l'Université Paul-Valéry. Tout compte resté sans mouvement pendant une période dépassant 6 mois sera automatiquement fermé.