

Charte informatique à destination des utilisateurs

Vu le code de l'éducation

Vu le code pénal

Vu le code de la propriété intellectuelle

Vu le code des postes et des communications électroniques

Vu la loi du 29 juillet 1881 sur la liberté de la presse

Vu la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés

Vu la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique

Préambule

L'Université met en œuvre des systèmes d'information (SI) nécessaires à l'exercice de ses missions.

Le réseau informatique de l'Université est relié par l'intermédiaire du Réseau RENATER (REseau NATIONAL de télécommunications pour la Technologie, l'Enseignement et la Recherche) à une communauté d'utilisateurs travaillant dans le domaine de l'éducation, de la culture, de la recherche et de la technologie.

La présente Charte définit les règles relatives à l'utilisation du réseau informatique, des ressources et services mis à disposition par l'Université et tend à sensibiliser les utilisateurs aux risques liés à leur utilisation en termes d'intégrité et de confidentialité des données traitées et de sécurité informatique.

Article 1. Champ d'application et définitions

1.1 Utilisateurs

La présente charte s'applique à l'ensemble des utilisateurs des SI de l'Université, quel que soit leur statut :

- Personnels et assimilés (agents, vacataires, stagiaires, personnels "invités" ou "hébergés", employés de sociétés prestataires ou hébergées ainsi que les visiteurs occasionnels) ;
- Usagers (étudiants, stagiaires de la formation continue, auditeurs libres).

1.2 Systèmes d'information

Les SI de l'Université sont notamment constitués par l'ensemble des moyens matériels, logiciels, applications, bases de données et réseaux de télécommunications, y compris l'informatique nomade ainsi que les téléphones fixes ou portables, pouvant être mis à disposition des Utilisateurs.

Pour des raisons de sécurité du réseau, est également considéré comme faisant partie du SI le matériel personnel des utilisateurs connecté au réseau de l'Université, ou contenant des informations à caractère professionnel concernant l'Université.

1.3 La direction en charge des systèmes d'information

La Direction des Systèmes d'Information (DSI) assure le bon fonctionnement et la sécurité des réseaux, des moyens informatiques et de communication de l'Université. Les personnels de la DSI disposent d'outils techniques afin de procéder aux investigations et au contrôle de l'utilisation des systèmes informatiques mis en place.

Ils ont accès à l'ensemble des données techniques et s'engagent à respecter les règles de confidentialité applicables aux contenus des documents. Ils sont assujettis au devoir de réserve et sont tenus de préserver la confidentialité des données qu'ils sont amenés à connaître dans le cadre de leurs fonctions. Ainsi, ils ne peuvent

divulguer les informations qu'ils sont amenés à connaître dans le cadre de leurs fonctions dès lors que ces informations relèvent de la vie privée de l'utilisateur et qu'elles ne mettent en cause ni le bon fonctionnement technique des applications, ni leur sécurité, et qu'elles ne tombent pas dans le champ de l'article 40 alinéa 2 du code de procédure pénale.

Article 2. Accès aux systèmes d'information

2.1 Conditions d'accès

L'utilisateur doit respecter les modalités de raccordement des matériels aux réseaux de communication telles qu'elles lui sont précisées par la DSI. Ces raccordements ne pourront pas être modifiés sans autorisation préalable.

Le droit d'accès à un système informatique est personnel et incessible. L'utilisateur est responsable de l'utilisation des ressources informatiques (locales ou distantes) effectuée à partir de son droit d'accès.

Le droit d'accès aux SI est temporaire, il est retiré dans les cas suivants :

- la fonction ou le statut de l'utilisateur ne le justifie plus ; il appartient alors à chaque utilisateur préalablement au retrait de son droit d'accès de détruire son espace de données à caractère privé, la responsabilité de l'administration ne pouvant être engagée quant à la conservation de cet espace ;
- non-respect de la présente Charte.

2.2 Utilisation conforme aux missions de l'Université

Les moyens informatiques sont mis à disposition des utilisateurs :

- à des fins professionnelles en ce qui concerne les personnels et assimilés ;

- à des fins liées à la pédagogie, à la recherche, à l'orientation ou à l'insertion professionnelle en ce qui concerne les usagers.

L'utilisation des moyens informatiques à des fins privées est tolérée sous réserve qu'elle soit non lucrative, raisonnable et limitée tant dans la fréquence que dans la durée. Elle ne doit pas nuire à la qualité du travail de l'utilisateur, au temps qu'il y consacre et au bon fonctionnement du service. Elle doit être conforme à la loi, l'ordre public et à la Charte déontologique RENATER disponible sur le site www.renater.fr

En toute hypothèse, le surcoût qui résulte de l'utilisation privée résiduelle des systèmes d'information doit demeurer négligeable au regard des coûts d'exploitation globaux.

Il appartient à l'utilisateur de mentionner expressément le caractère privé de ses données à caractère privé (mention « privé » dans le titre) et de procéder à leur stockage dans un répertoire de données nommé « Privé ». Ce répertoire ne sera alors pas (systématiquement) inclus dans les sauvegardes. La sauvegarde régulière incombera à l'utilisateur, sous sa seule responsabilité.

Pour les personnels de l'Université, les données dont le caractère privé n'est pas expressément mentionné sont réputées à caractère professionnel. L'université peut y avoir accès, pour les besoins du service, même sans l'accord des personnes concernées.

Afin d'assurer la continuité du service et de garantir l'accès à leurs données professionnelles, les personnels utilisent, dans la mesure du possible, les espaces de stockage partagés mis à leur disposition. Ces espaces de stockage ne sont utilisés que pour un usage professionnel et ne peuvent être verrouillés que par des mots de passe fonctionnels à usage du service.

2.3 Paramètres d'accès

L'accès à certains éléments du SI est protégé par des paramètres de connexion (identifiants, mots de passe).

Ces paramètres sont personnels à l'utilisateur et doivent être gardés confidentiels. Ils permettent en particulier que les actions qu'il mène au sein des systèmes soient identifiables.

Ces paramètres ne doivent pas être transmis à des tiers ou aisément accessibles. Ils doivent être saisis par l'utilisateur à chaque accès et ne pas être conservés en mémoire dans le SI. L'attention des utilisateurs est attirée sur le fait que la DSI ne demandera en aucun cas (quel que soit le moyen utilisé : mail, téléphone, courrier...) la communication de ces paramètres.

Ces paramètres doivent respecter un certain degré de robustesse. Des consignes de sécurité sont élaborées régulièrement par le responsable de la sécurité des systèmes d'information (RSSI) afin de recommander les bonnes pratiques en la matière.

Article 3. Protection des données à caractère personnel

La loi n°78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés définit les conditions dans lesquelles des traitements de données à

caractère personnel peuvent être effectués. Elle ouvre aux personnes concernées par les traitements un droit d'accès et de rectification des données enregistrées sur leur compte.

L'Université a désigné un correspondant à la protection des données à caractère personnel. Ce dernier a pour mission de veiller au respect des dispositions de la loi n°78-17 du 6 janvier 1978 modifiée. Il est obligatoirement consulté par le responsable des traitements préalablement à leur création. Il recense dans un registre la liste de l'ensemble des traitements de données à caractère personnel de l'Université au fur et à mesure de leur mise en œuvre. Cette liste est tenue à disposition de toute personne en faisant la demande.

Le correspondant veille au respect des droits des personnes (droit d'accès, de rectification et d'opposition). En cas de difficultés rencontrées lors de l'exercice de ces droits, les personnes concernées peuvent saisir le correspondant (cil@univ-lyon2.fr).

Article 4. Règles d'utilisation des systèmes d'information

4.1 Sécurité

Les utilisateurs sont tenus de participer à la sécurité du système et des données en respectant les règles de sécurité minimales suivantes :

- toute installation de logiciel supplémentaire est subordonnée à l'accord de la DSI. Les utilisateurs ne doivent pas modifier les paramètres du poste de travail ;
- l'utilisation de solutions externes de messagerie et de stockage en ligne est prohibée pour les personnels. De manière générale, l'utilisation de services externes gratuits, qui peuvent exposer de façon incontrôlée des données sensibles, est fortement déconseillée. Les solutions et services numériques proposés par la DSI doivent toujours être privilégiés. En cas de stockage externe de données de l'établissement, le contrat avec l'hébergeur doit garantir la sécurité, la confidentialité et l'intégrité des données conformément aux dispositions de la loi informatique et libertés.

Les utilisateurs ne doivent pas effectuer d'expérimentation sur la sécurité des SI et réseaux, ni sur les virus informatiques sans autorisation préalable de la DSI.

Tout utilisateur d'un réseau informatique s'engage à ne pas effectuer d'opérations qui pourraient avoir pour conséquence :

- d'interrompre le fonctionnement du réseau ou d'un système connecté au réseau ;
- d'accéder aux informations privées d'autres utilisateurs sur le réseau ;
- de nécessiter la mise en place de moyens humains ou techniques supplémentaires pour son contrôle.

4.2 Utilisation d'équipements nomades

On entend par « équipements nomades » tous les moyens techniques mobiles (ordinateur portable, imprimante

portable, téléphones mobiles, CD ROM, clé USB, carte mémoire etc.).

Quand cela est techniquement possible, ils doivent faire l'objet d'une sécurisation particulière, au regard de la sensibilité des documents qu'ils peuvent stocker, notamment par chiffrement.

L'utilisation d'équipements nomades pour relever automatiquement la messagerie électronique comporte des risques particuliers pour la confidentialité des messages, notamment en cas de perte ou de vol de ces équipements. Quand ces appareils ne sont pas utilisés pendant quelques minutes, ils doivent donc être verrouillés par un moyen adapté de manière à prévenir tout accès non autorisé aux données qu'ils contiennent.

L'utilisateur d'applications mobiles de messagerie s'assurera que ces applications n'utilisent pas de serveurs intermédiaires entre leur terminal et les serveurs de messagerie de l'établissement. La liste des applications validées est disponible auprès du RSSI.

4.3 Gestion des ressources

Les utilisateurs doivent respecter les règles et procédures mises en place pour l'acquisition et la sortie des données sur les matériels de l'Université.

4.4 Respect des droits des tiers

4.4.1 Respect du caractère confidentiel des informations

L'utilisateur respecte les contenus à caractère confidentiel, et s'engage particulièrement :

- A ne pas lire, copier, divulguer ou modifier les fichiers d'un autre utilisateur sans y avoir été explicitement autorisé par son propriétaire et/ou son auteur,
- A ne pas intercepter, détourner, utiliser ou divulguer les communications entre tiers.

4.4.2 Respect de la propriété intellectuelle

Les utilisateurs doivent s'abstenir de copier, diffuser ou reproduire tout logiciel ou document protégé par le droit d'auteur. Ils utilisent les logiciels et données conformément aux licences souscrites.

De manière générale, les utilisateurs s'assurent que les données qu'ils diffusent sur Internet ou qu'ils téléchargent ne portent pas atteinte aux droits des tiers (droit d'auteur, droit des marques, droit au respect de la vie privée etc.).

4.4.3 Respect du droit des personnes

Il est interdit à tout utilisateur de porter atteinte à la vie privée d'autrui par un procédé quelconque et notamment par la transmission sans son consentement de son image ou de ses écrits diffusés à titre confidentiel ou privé. De manière générale, l'utilisateur veille au respect de la personnalité, de l'intimité et de la vie privée d'autrui, notamment des mineurs.

4.4.4 Respect des clauses contractuelles

Les utilisateurs doivent respecter les conditions contractuelles notamment prévues pour l'usage des

ressources documentaires électroniques et en avoir un usage raisonnable, personnel et strictement non commercial.

4.4.5 Respect d'un comportement correct

Un utilisateur ne doit pas utiliser les systèmes informatiques pour harceler d'autres utilisateurs par des communications non souhaitées par les tiers ou pour afficher/diffuser des informations illégales.

Il est également interdit de consulter, charger, stocker, diffuser via les moyens informatiques des documents, informations, images, fichiers... contraires à la loi ou à l'ordre public et plus particulièrement à caractère violent, pornographique, incitant au racisme ou à la violence, portant atteinte au respect de la personne humaine et de sa dignité ainsi qu'à la protection des mineurs ; de caractère diffamatoire ou injurieux et de manière générale illicite.

4.5 Respect de la déontologie informatique

Les utilisateurs ne doivent pas effectuer de manœuvres qui auraient pour objet de méprendre les autres utilisateurs sur leur identité.

Les utilisateurs doivent respecter les procédures d'authentification en vigueur de façon à ce que les actions qu'ils mènent au sein des systèmes soient identifiables.

Article 5. Comptes de messagerie

Outre l'ensemble des dispositions de la présente Charte, les dispositions suivantes s'appliquent spécifiquement aux comptes de messagerie.

5.1 Mise à disposition d'un compte de messagerie

Les agents de l'Université et les étudiants disposent d'une adresse de messagerie électronique attribuée par l'Université. L'adresse électronique de l'utilisateur est nominative.

Les messages électroniques reçus sur cette messagerie font l'objet d'un contrôle antiviral et d'un filtrage anti-spam. Les titulaires d'un compte de messagerie sont invités à informer le support utilisateur de la DSI des dysfonctionnements qu'ils constatent dans le dispositif de filtrage.

Dans leur pratique professionnelle, les agents de l'Université et les étudiants utilisent la messagerie électronique mise à disposition par l'Université ou à défaut par des partenaires institutionnels. L'utilisation d'un service de messagerie d'un fournisseur extérieur à l'université dans un contexte professionnel, de même que les transferts de messagerie institutionnelle vers un service de messagerie extérieur à l'université, sont proscrits, sauf s'il s'agit du service de messagerie institutionnel d'un autre établissement public.

L'adresse de messagerie professionnelle ne peut pas être utilisée par les agents et les étudiants pour s'inscrire sur des sites à usage non professionnel.

S'agissant des comptes de messagerie attribués aux agents, tout message est réputé à caractère professionnel sauf si son caractère personnel est expressément signalé (mention « personnel » ou « privé » dans son objet).

5.2 Suppression du compte de messagerie

La messagerie n'est mise à disposition des utilisateurs que tant que leur statut le justifie.

L'utilisateur pourra demander à accéder aux données de son compte pendant une durée de trois mois après son départ définitif afin de détruire ou récupérer ses données à caractère privé. Au-delà, les données de cet espace seront détruites. S'agissant des comptes de messagerie professionnels, l'Université se réserve le droit de consulter les messages à caractère professionnel avant la suppression du compte.

5.3 Listes de diffusion

La création de listes de diffusion institutionnelles doit avoir pour objet la communication et l'information des personnels et des usagers dans le cadre de l'activité et des missions de l'Université. La création de listes institutionnelles répondant à d'autres finalités est proscrite en l'absence d'accord explicite des intéressés.

La constitution de listes de diffusion à partir des adresses mail personnelles des agents ou des étudiants est proscrite sans le consentement express des destinataires.

Article 6. Administration du système d'information

Afin de surveiller le fonctionnement et de garantir la sécurité du système d'information de l'Université, différents dispositifs sont mis en place.

6.1. Les systèmes automatiques de filtrage

A titre préventif, des systèmes automatiques de filtrage permettant de diminuer les flux d'information pour l'Université, et d'assurer la sécurité et la confidentialité des données sont mis en œuvre.

Il s'agit notamment du filtrage des sites Internet, de l'élimination des courriels non sollicités, du blocage de certains protocoles (peer to peer, messagerie instantanée...).

6.2. Les systèmes automatiques de traçabilité

6.2.1 Finalités

L'Université met en œuvre un système de traitement des fichiers de journalisation (fichiers « logs ») à des fins :

- de sécurité (détection et analyse d'anomalies ou d'incidents de sécurité) et de détection des abus ;
- d'établissement de statistiques et d'indicateurs visant à optimiser et faire évoluer les SI¹ ;
- de mise à disposition des fichiers sur réquisition judiciaire.

6.2.2 Catégories de données

Ces fichiers comportent les données suivantes : informations permettant l'identification de l'utilisateur, données relatives aux équipements utilisés, caractéristiques techniques, date, heure et durée de

chaque communication, données relatives aux services complémentaires demandés ou utilisés et leurs fournisseurs, données permettant d'identifier le ou les destinataires.

6.2.3 Durée de conservation

La durée de conservation des journaux informatiques est d'un an maximum. L'Université s'interdit de les exploiter au-delà de 3 mois sauf sur réquisition officielle ou sous une forme rendue anonyme.

6.3. Gestion du poste de travail

À des fins de maintenance informatique, le service informatique interne de l'Université peut accéder à distance à l'ensemble des postes de travail. Cette intervention s'effectue avec l'autorisation expresse de l'utilisateur. Dans le cadre de mises à jour et évolutions du système d'information, et lorsqu'aucun utilisateur n'est connecté sur son poste de travail, le service informatique peut être amené à intervenir sur l'environnement technique des postes de travail. Il s'interdit d'accéder aux contenus.

Article 7. Sanctions

Le manquement aux règles et mesures de sécurité de la présente charte est susceptible d'engager la responsabilité de l'utilisateur.

La présidence de l'Université peut prendre toute mesure conservatoire à l'encontre d'un utilisateur (suspension des droits d'accès, suppression d'une page web hébergée...) sans préjudice d'éventuelles procédures disciplinaires ou pénales.

Article 8. Entrée en vigueur

La présente charte a été approuvée par :

- la commission de la formation et de la vie universitaire du conseil académique de l'Université le/.../....
- le conseil d'administration de l'Université le .../.../...

Elle est annexée au règlement intérieur. Elle annule et remplace...

¹ Exemples : statistiques de fréquentation des portails institutionnels, rubriques de l'intranet les plus visitées, qualité des emails reçus (spam, non-spam, douteux, virus...) en fonction du temps, taux d'utilisation des différents outils du bureau virtuel etc.