Charte informatique des personnels

1. Préambule

La présente Charte a pour objet de formaliser les règles de déontologie et de sécurité que l'«utilisateur» s'engage à respecter en contrepartie de la mise à disposition des ressources informatiques de l'institution. Cette charte est portée à la connaissance des «utilisateurs». Par «utilisateur», on entend : toute personne ayant accès, dans le cadre de l'exercice de son activité professionnelle, aux moyens informatiques et de télécommunications quel que soit son statut et notamment :

- les agents titulaires et non titulaires concourant à l'exécution des missions du service public de l'enseignement supérieur et de la recherche ;
- le personnel des prestataires de service dont le contrat passé avec le ministère ou le service concerné le prévoit expressément;
- et plus généralement toute personne ayant accès aux systèmes d'information relevant du ministère chargé de l'Éducation nationale, de l'enseignement supérieur et de la recherche.

La Charte définit le comportement loyal, respectueux et responsable que chacun s'oblige à adopter à l'occasion de l'utilisation des ressources informatiques de l'institution.
L'utilisation du système d'information suppose le respect des règles visant à assurer la sécurité, la performance des traitements, la préservation des données confidentielles et le respect des dispositions légales et réglementaires qui s'imposent.

Tout «utilisateur» est responsable, en tout lieu, de l'usage qu'il fait des ressources informatiques, de télécommunications et des réseaux auxquels il a accès.
L'administration est tenue de respecter la vie privée de ses agents.

2. Champ d'application

2.1 Périmètre

Les règles de déontologie et de sécurité figurant dans la présente Charte, de même que l'obligation de respecter la législation en vigueur s'appliquent à l'ensemble des «utilisateurs». Les «administrateurs» des systèmes d'information sont soumis en qualité d'«utilisateurs» à la présente Charte.

2.2 Systèmes d'information

Il s'agit de l'ensemble des moyens matériels, logiciels, applications et réseaux de télécommunications (Réseau Privé Virtuel, Réseau Téléphonique Commuté, etc.) pouvant être mis à disposition de l'«utilisateur», y compris via l'informatique nomade tels que les assistants personnels, les ordinateurs portables, les téléphones portables, etc.

3. Destination des systèmes d'information

3.1 Utilisation professionnelle / privée

Les moyens informatiques mis à disposition de l'utilisateur sont prioritairement à usage professionnel.
L'espace privé doit être clairement affiché comme tel et rester limité. Les personnels du service informatique doivent pouvoir intervenir sur toute la partie professionnelle même en l'absence de l'utilisateur.

L'usage de cet outil à des fins non professionnelles est une tolérance. Les abus: activités ludiques ou commerciales, communications à caractère politique ou religieux sont susceptibles de faire l'objet d'une procédure disciplinaire ;

3.2 Utilisation des ressources des systèmes d'information

Les ressources matérielles nomades mises à la disposition de l'«utilisateur» par l'administration, doivent faire l'objet d'une attestation de remise signée par l'«utilisateur». L'«utilisateur» a l'obligation de préservation du matériel qui lui est confié. En cas de dysfonctionnement de l'appareil mis à disposition, le service informatique a pour seule obligation de le remettre en son état initial, sans qu'il puisse lui être imputé des pertes de données.

3.3 Gestion des départs

Il appartient à l'«utilisateur», lors de son départ définitif du service ou de l'établissement, de détruire son espace «privé».
La responsabilité de l'administration ne pourra être engagée quant à la conservation et la confidentialité de l'espace privé d'un «utilisateur» quittant le service ou l'établissement.

4. Sécurité

4.1 Règles de sécurité

Les niveaux d'accès ouverts à l'«utilisateur» sont définis en fonction du «profil» qui est établi pour lui selon les critères propres à son statut, sa mission, la nature de son poste et ses besoins professionnels.
La sécurité des moyens informatiques mis à la disposition de l'«utilisateur» lui impose :

- de respecter les consignes de sécurité et notamment les règles relatives à la définition et aux changements des mots de passe;
- de respecter la gestion des accès, en particulier ne pas utiliser les noms et mot de passe d'un autre «utilisateur», ni chercher à connaître ces informations ;
- de garder strictement confidentiels ses mots de passe et ne pas les dévoiler à un tiers.

Si pour des raisons exceptionnelles et ponctuelles, un «utilisateur» se trouvait dans l'obligation de communiquer son mot de passe, il devrait procéder, dès qu'il en a la possibilité, au changement de ce dernier ou en demander la modification à «l'administrateur» du réseau. Le bénéficiaire de la communication du mot de passe ne peut le communiquer à son tour à un tiers, ni l'utiliser en dehors de la circonstance exceptionnelle à l'origine de la communication.

L'«utilisateur» est informé que les mots de passe constituent une mesure de sécurité destinée à éviter les utilisations malveillantes ou abusives, de protéger la confidentialité des données, d'assurer l'identification des connexions. Cette mesure ne confère pas aux outils informatiques protégés un caractère personnel.

L'utilisateur est informé que son mot de passe est personnel et incessible. Son usage à valeur de preuve de son utilisation « personnelle » de ressources informatiques. Tout usage de son mot de passe engage donc sa responsabilité personnelle.

Par ailleurs, la sécurité des ressources mises à la disposition de l'«utilisateur» nécessite:

- de verrouiller son poste de travail en cas d'absence et d'utiliser les économiseurs d'écran avec mot de passe afin de préserver l'accès à son poste de travail.
- d'avertir immédiatement ou dans le délai le plus court, sa hiérarchie de tout dysfonctionnement constaté, de toute anomalie découverte telle une intrusion dans le système d'information, etc.… ;
- de ne pas modifier l'équipement qui lui est confié en conformité avec les dispositions en vigueur de l'établissement ;
- de ne pas connecter aux réseaux locaux des matériels non autorisés par l'institution ;
- de ne pas installer, télécharger ou utiliser sur les matériels informatiques de logiciels ou progiciels sans qu'une licence d'utilisation appropriée n'ait été souscrite par l'établissement ;
- de s'interdire d'accéder ou tenter d'accéder à des ressources ou programmes informatiques pour lesquels l'«utilisateur» ne bénéficie pas d'une habilitation expresse : l'«utilisateur» doit

limiter ses accès aux seules ressources pour lesquelles il est expressément habilité à l'exclusion de toutes autres, même si cet accès est techniquement possible;

- de signaler au RSII ou bien à la Personne Juridiquement Responsable (PJR) tout accès à une ressource informatique qui ne corresponde pas à son habilitation: l'«utilisateur» s'interdit toute divulgation de cette possibilité d'accès.

L'« utilisateur » est informé que pour des raisons d'administration des systèmes et de gestion de la sécurité, les administrateurs systèmes ont la possibilité de réaliser des interventions à distance pour assurer la maintenance corrective ou évolutive des Systèmes d'Information mis à leur disposition ainsi que pour préserver ou renforcer des mesures de sécurité.

4.2 Mesures de contrôle de la sécurité

Le système d'information ainsi que l'ensemble des moyens de communication peuvent donner lieu à une surveillance et un contrôle à des fins statistiques, de traçabilité, d'optimisation, de sécurité et de détection des abus. Les personnels en charge de ces opérations sont soumis au secret professionnel et ne peuvent divulguer les informations qu'ils sont amenés à connaître dans le cadre de leur fonction, en particulier lorsque ces informations sont couvertes par le secret des correspondances ou relèvent de la vie privée de l'«utilisateur» et lorsque ces informations ne remettent pas en cause ni le bon fonctionnement technique des applications, ni leur sécurité, ni l'intérêt du service.
Le service informatique est le seul utilisateur de ces informations qui sont effacées à l'expiration d'un délai de trois mois.

4.3. Sécurité antivirale

L'«utilisateur» doit se conformer aux règles liées à la mise en œuvre au sein de l'institution, des dispositifs de lutte contre les virus et attaques logiques informatiques. L'«utilisateur» est informé que toute information bloquante ou présentant une difficulté technique d'acheminement à son destinataire, peut être isolée voire détruite.
Les administrateurs sont autorisés, en cas de difficultés majeures, à arrêter les services réseaux.

5. Messagerie électronique

L'administration met à la disposition de l'«utilisateur» une boîte à lettres professionnelle nominative qui lui permet d'émettre et de recevoir des messages électroniques.
L'utilisation de la messagerie constitue l'un des éléments essentiels d'optimisation du travail au sein de l'institution et de la politique de mutualisation de l'information. L'élément nominatif de l'adresse de la messagerie qui constitue le prolongement de l'adresse administrative, n'a pas pour effet de retirer le caractère professionnel de la messagerie.

5.1 Boîte aux lettres

Chaque «utilisateur» peut autoriser, à son initiative et sous sa responsabilité, l'accès par des tiers à sa boîte de réception.
L'attribution de boîtes générales fonctionnelles ou organisationnelles par service ou groupe d'«utilisateurs» est possible.
Les listes de diffusion institutionnelles désignant une catégorie ou un groupe d'«utilisateurs» ne peuvent être mises en place et utilisées que sous la condition d'une autorisation de l'institution.

5.2 Contenu des messages électroniques

Les messages électroniques permettent d'échanger des informations à vocation professionnelle liées à l'activité directe de l'institution. En toutes circonstances, l'«utilisateur» doit adopter un comportement loyal et digne.
En cas de difficulté, les administrateurs systèmes se réservent le droit de supprimer tout message bloquant.

Tout message à caractère privé, reçu ou émis, doit comporter une mention particulière explicite indiquant le caractère privé dans la zone «sujet». À défaut, le message sera réputé professionnel.
Sont interdits les messages à caractère injurieux, raciste, discriminatoire, insultant, dénigrant, diffamatoire, dégradant ou susceptibles de révéler les opinions politiques, religieuses, philosophiques, les mœurs, l'appartenance syndicale, la santé des personnes ou encore, de porter atteinte à leur vie privée ou à leur dignité ainsi que les messages portant atteinte à l'image, la réputation ou à la considération du service public..

5.3 Émission et réception des messages

L'«utilisateur» doit s'assurer de l'identité et de l'exactitude des adresses des destinataires des messages. Il doit veiller à ce que la diffusion des messages soit limitée aux seuls destinataires concernés afin d'éviter la diffusion de messages en masse, l'encombrement inutile de la messagerie ainsi qu'une dégradation du service.

5.4 Statut et valeur juridique des messages

Les messages électroniques échangés avec des tiers peuvent, au plan juridique, former un contrat, constituer une preuve ou un commencement de preuve. L'«utilisateur» doit en conséquence être vigilant sur la nature des messages électroniques qu'il échange au même titre que les courriers traditionnels.

5.5 Stockage et archivage des messages électroniques

En cas d'archivage automatique des messages les utilisateurs doivent en outre être informés des modalités de l'archivage, de la durée de conservation des messages et des modalités d'exercice de leur droit d'accès.
Chaque «utilisateur» doit organiser et mettre en œuvre les moyens nécessaires à la conservation des messages pouvant être indispensables ou simplement utiles en tant qu'éléments de preuve.
À ce titre, il doit notamment se conformer aux règles définies dans la présente Charte pour l'utilisation des technologies de l'information et de communications en vigueur.

5.6 Gestion des absences

En cas d'absence d'un «utilisateur», toute mesure visant à assurer la continuité du service pourra être mise en œuvre par la hiérarchie. L'agent concerné sera informé dès que possible de la liste des messages transférés.

6. Web Internet et traces

L'accès à Internet n'est autorisé qu'au travers des dispositifs de sécurité mis en place par l'institution. Il est rappelé que le réseau Internet se trouve soumis à l'ensemble des règles de droit. L'«utilisateur» qui dispose d'un accès au réseau Internet est informé des risques et limites inhérents à son utilisation.
L'institution a mis en place un système permettant d'assurer la traçabilité des accès Internet et des données échangées. Elle se réserve le droit de procéder à un filtrage des sites, au contrôle à posteriori des sites, des pages visitées et durées des accès correspondants.
Les traces correspondantes aux connexions et à l'accès aux serveurs web et aux ressources informatiques en général accédés par l'ensemble des utilisateurs sont conservées et font l'objet d'une déclaration auprès de la CNIL.

7. Téléchargements - logiciels

Le téléchargement de fichiers, notamment de sons et d'images, depuis le réseau Internet est autorisé dans le respect des droits de la propriété intellectuelle telle qu'elle est définie à l'article 10 mais doit correspondre à l'activité professionnelle de l'«utilisateur». Cependant, l'administration se réserve le droit de limiter à priori le téléchargement de certains fichiers pouvant se révéler volumineux ou comporter des virus susceptibles d'altérer le bon fonctionnement du système d'information de l'institution.

8. Confidentialité - discrétion

Chaque «utilisateur» a une obligation de confidentialité et de discrétion à l'égard des informations et documents électroniques à caractère confidentiel auxquels il a accès dans le système d'information.
Le respect de cette confidentialité implique notamment :

- de veiller à ce que les tiers non autorisés n'aient pas connaissance de telles informations ;
- de respecter les règles d'éthique professionnelle et de déontologie, ainsi que l'obligation de réserve et le devoir de discrétion.

9. Propriété intellectuelle

L'utilisation des moyens informatiques implique le respect des droits de propriété intellectuelle de l'institution, de ses partenaires et plus généralement de tous tiers titulaires de tels droits. En conséquence, chacun doit :

- utiliser les logiciels dans les conditions des licences souscrites ;
- ne pas reproduire, copier, diffuser, modifier et utiliser les logiciels, bases de données, pages web, textes, images, photographies ou autres créations protégées par le droit d'auteur ou un droit privatif sans avoir obtenu préalablement l'autorisation des titulaires de ces droits.

10. Respect de la loi informatique et libertés

L'université de Nîmes 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.
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 peuvent saisir le correspondant à l'adresse internet suivante : cil@unimes.fr
L'utilisateur est informé de la nécessité de respecter les dispositions légales en matière de traitement automatisé des données à caractère personnel.
Par données à caractère personnel, il y a lieu d'entendre, les informations qui permettent - sous quelque forme que ce soit - directement ou indirectement, l'identification des personnes physiques auxquelles elles s'appliquent telles que par exemple les adresses électroniques.
Toutes les créations de fichiers comprenant ce type d'informations, y compris lorsqu'elles résultent de croisement ou d'interconnexion de fichiers préexistants, sont soumises aux formalités préalables prévues par la loi n° 78-17 du 06 janvier 1978 modifiée par la loi n° 2004-801 du 6 août 2004. En conséquence, tout «utilisateur» souhaitant procéder à un tel traitement devra en informer préalablement le correspondant informatique et libertés.

11. Limitations des usages

En cas de non-respect des règles définies dans la présente Charte, la «Personne Juridiquement Responsable» pourra, sans préjuger des poursuites ou procédures de sanctions pouvant être engagées à l'encontre des personnels, limiter les usages par mesure conservatoire.
Par «Personne Juridiquement Responsable», on entend : toute personne ayant la responsabilité de représenter le l'Etat au sein d'un établissement d'enseignement supérieur et de recherche (président d'université, vice- président, directeur général des services).

12. Entrée en vigueur de la charte

La présente Charte est annexée au règlement intérieur de l'Université de Nîmes.

Le présent document annule et remplace tous autres documents ou chartes afférents à l'utilisation des Systèmes d'Information.

Je, soussigné, (nom prénom)…….....

déclare :

Accepter (*)

la charte informatique de l'Université de Nîmes

Refuser (*)

Le Signature

Annexe A. règles de création de mots de passe

Les mots de passe doivent :

- Comporter 8 caractères
- Ne pas être un mot présent dans un dictionnaire (quelle que soit la langue)
- Ne pas être une permutation d'un mot présent dans un dictionnaire (quelle que soit la langue)
- Ne pas être une information se rapportant directement au titulaire du compte (date de naissance, nom d'animal de compagnie.)
- Comporter au moins 2 chiffres
- Comporter de préférence 2 caractères spéciaux (non contigus).

Annexe B. Règles de création de nom d'URL pour une association

Le nom d'Url doit être conforme au format suivant :

www.assoc-<nomassociation>.unimes.Fr