Charte informatique KAMENETWORK

Préambule

Le "système d'information" recouvre l'ensemble des ressources matérielles, logicielles, applications, bases de données et réseaux de télécommunications, pouvant être mis à disposition par l'institution.

L'informatique nomade, tels que les assistants personnels, les ordinateurs portables, les téléphones sont également un des éléments constitutifs du système d'information.

On désignera par « services internet » : la mise à disposition par des serveurs locaux ou distants de moyens d'échanges et d'informations diverses : web, messagerie, téléphonie sur IP, visioconférence...

Par « institution » il faut entendre l'ensemble des Etablissement gérés par KameNetwork (Kamen Marseille-Luminy, Kamen Gap, …)
Le terme d'« utilisateur » recouvre toute personne ayant accès aux ressources du système d'information quel que soit son statut.

Il s'agit notamment de :

- tout agent titulaire ou non titulaire concourant à l'exécution dos missions du service public de l'enseignement supérieur et de la recherche ;
- tout prestataire ayant contracté avec l'institution.

Le bon fonctionnement du système d'information (SI) suppose le respect des dispositions législatives et réglementaires, notamment le respect des règles visant à assurer la sécurité, la performance des traitements et la conservation des données.

La présente charte définit les règles d'usages et de sécurité que l'institution et l'utilisateur s'engagent à respecter : **elle précise les droits et devoirs de chacun**.

La charte est accompagnée d'un guide juridique qui rappelle les dispositions législatives et réglementaires en vigueur pour son application. Elle peut être complétée par des guides d'utilisation définissant les principales règles et pratiques d'usage.

L'institution porte à la connaissance de l'utilisateur la présente charte.

1) Engagements de l'institution

L'institution met en œuvre les mesures nécessaires pour assurer la sécurité et le bon fonctionnement du système d'information et la protection des utilisateurs ainsi que de leurs données personnelles.

L'institution facilite l'accès des utilisateurs aux ressources du système d'information. Les ressources mises à leur disposition sont prioritairement à usage professionnel mais l'institution est tenue de respecter l'utilisation résiduelle du système d'information à titre privé.

2) Engagements de l'utilisateur

L'utilisateur est responsable, en tout lieu, de l'usage qu'il fait du système d'information auquel il a accès. Il a une obligation de réserve et de confidentialité à l'égard des informations et documents auxquels il

accède. Cette obligation implique le respect des règles d'éthique professionnelle et de déontologie. (Voir annexe juridique).

Les utilisateurs ont une responsabilité particulière dans l'utilisation qu'ils font des ressources mises à leur disposition par l'institution.

En tout état de cause, l'utilisateur est soumis au respect des obligations résultant de son statut ou de son contrat.

I. Champ d'application

Les règles d'usage et de sécurité figurant dans la présente charte s'appliquent à l' institution ainsi qu'à l'ensemble des utilisateurs.

Les usages relevant de l'activité des organisations syndicales sont régis par l'accord relatif à l'usage des listes de diffusion par les organisations syndicales.

II. Conditions d'utilisation du système d'information

1) Utilisation Professionnelle / privée

Le système d'information (messagerie, internet est un outil de travail ouvert à des usages professionnels administratifs, pédagogiques et de recherche.

Il peut également constituer le support d'une communication privée dans les conditions décrites ci-dessous.

L'utilisation résiduelle du système d'information à titre privé doit être non lucrative et raisonnable, tant dans sa fréquence que dans sa durée. En toute hypothèse, le surcoût qui en résulte doit demeurer négligeable au regard du coût global d'exploitation

Cette utilisation ne doit pas nuire à la qualité du travail de l'utilisateur, au temps qu'il y consacre et au bon fonctionnement du service.

Toute information est réputée professionnelle à l'exclusion des données explicitement désignées par l'utilisateur comme relevant de sa vie privée. Ainsi, il appartient à l'utilisateur de procéder au stockage de ses données à caractère privé dans un espace de données prévu explicitement à cet effet ou en mentionnant le caractère privé sur la ressource. La sauvegarde régulière des données à caractère privé incombera à l'utilisateur.

L'utilisation du système d'information à titre privé doit respecter les lois et la réglementation en vigueur. Conformément aux dispositions du code pénal, l'utilisateur ne doit pas diffuser des informations ou données dont le contenu présente un caractère illégal, notamment raciste, diffamatoire ou injurieux. Ceci s'applique tant aux fichiers qu'aux messages avec ou sans pièces attachées quelle que soit la forme des contenus (textuels, sonores, audiovisuels ou multimédias).

La consultation de sites de contenus à caractère pornographique depuis les locaux de l'institution est interdite

2) Continuité de service : gestion des absences et des départs

Aux seules fins d'assurer la continuité de service, l'utilisateur informe sa hiérarchie des modalités permettant l'accès aux ressources mises spécifiquement à sa disposition, En cas d'absence, toute mesure visant à garantir la continuité du service public peut être prise par l'université.

L'utilisateur est responsable de son espace de données à caractère privé. Lors de son départ définitif du service ou de l'établissement\ il lui appartient de détruire son espace de données à caractère privé, la responsabilité de I 'administration ne pouvant être engagée quant à la conservation de cet espace. Les mesures de conservation des données professionnelles sont définies avec le responsable désigné au sein de l'institution.

III. Principes de sécurité

1) Règles de sécurité applicables

L'institution met en œuvre les mécanismes de protection appropriés sur le système d'information mis à la disposition des utilisateurs.

L'utilisateur est informé que les codes d'accès constituent une mesure de sécurité destinée à éviter toute utilisation malveillante ou abusive. Cette mesure ne confère pas aux outils informatiques protégés, un caractère personnel.

Les niveaux d'accès ouverts à l'utilisateur sont définis en fonction de la mission qui lui est conférée. La sécurité du système d'information mis à sa disposition lui impose de respecter les consignes de sécurité, notamment les règles relatives à la gestion des codes d'accès :

- de garder strictement confidentiels son (ou ses) codes d'accès et ne pas le(s) divulguer à un tiers ;
- de respecter la gestion des accès, en particulier ne pas utiliser les codes d'accès d'un autre utilisateur, ni chercher à les connaître.

Si pour des raisons exceptionnelles et ponctuelles, un utilisateur se trouve dans l'obligation de communiquer son mot de passe, il devra procéder, dès que possible, au changement de ce dernier ou en demander la modification à l'administrateur. 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.

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

- de la part de l'institution :
    - veiller à ce que les ressources sensibles ne soient accessibles qu'aux personnes habilitées, en dehors des mesures d'organisation de la continuité du service mises en place par la hiérarchie, et limiter l'accès aux seules ressources pour lesquelles l'utilisateur est expressément habilité
- de la part de l'utilisateur :
    - respecter les règles **minimales** suivant pour la création des mots de passe :
        - 12 caractères minimum
        - Au moins une majuscule (de préférence pas au début du mot de passe), une minuscule, un chiffre, un caractère spécial
        - Renouvelé tous les 6 mois
        - Il doit être fondamentalement différent des 15 anciens mots de passes utilisés

- s’interdire d’accéder ou de tenter d’accéder à des ressources du système d’information, pour lesquelles il n’a pas reçu d’habilitation explicite ;
- ne pas connecter directement aux réseaux locaux des matériels autres que ceux confiés ou autorisés par l’institution, ou ceux dont la liste a été précisée dans un guide d’utilisation établi par le service ou l’établissement.
- en particulier, l’utilisation des ressources informatiques partagées de l’institution et la connexion d’un équipement privé et extérieur (tels qu’un ordinateur, commutateur, modem, borne d’accès sans fil...) sur le réseau sont interdites par défaut, sauf autorisation du responsable de l’institution,
- Ces autorisations sont strictement personnelles et ne peuvent en aucun cas être cédées, même temporairement à un tiers. Elles peuvent être retirées à tout moment. Toute autorisation prend fin lors de la cessation de l’activité professionnelle qui lia justifiée.
- ne pas installer, télécharger ou utiliser sur le matériel de l’institution, des logiciels ou progiciels dont les droits de licence n’ont pas été acquittés, ou ne provenant pas de sites dignes de confiance, ou sans autorisation de l’institution.
- se conformer aux dispositifs mis en place par l’institution pour lutter contre les virus et attaques par programmes informatiques
- assurer la protection de ses informations et plus particulièrement celtes considérées comme sensibles au sens de la politique de sécurité du système d’information (PSSI de l’institution) En particulier, il ne doit pas transporter sans protection (telle qu’un chiffrement) des données sensibles sur des supports non fiabilisés tels que ordinateurs portables, clés USB, disques externes, etc. Les supports qualifiés d’« informatique nomade » introduisent une vulnérabilité des ressources informatiques et comme tels doivent être soumis aux règles de sécurité de l’institution et à une utilisation conforme aux dispositions de la présente charte.
- en cas d’accès distant au S.I., prendre toutes la précaution nécessaire à la non divulgation de son mot de passe et des données auxquelles il a accès, en cohérence avec la PSSI de l’institution

2) Devoirs de signalement et d’information

L’institution doit porter à la connaissance de l’utilisateur tout élément susceptible de lui permettre d’apprécier le niveau de risque encouru dans l’utilisation du système d’information.

L’utilisateur doit avertir sa hiérarchie dans les meilleurs délais de tout dysfonctionnement constaté ou de toute anomalie découverte telle une intrusion dans le système d’information, etc. Il signale également à la personne responsable du site toute possibilité d’accès à une ressource qui ne correspond pas à son habilitation.

3) Mesures de contrôle de la sécurité

L’utilisateur est informé :

- que pour effectuer la maintenance corrective, curative ou évolutive, l’institution se réserve la possibilité de réaliser des interventions (le cas échéant à distance) sur les ressources mises à sa disposition ;
- qu’une maintenance à distance est précédée d’une information de l’utilisateur ;
- que toute information bloquante pour le système ou générant une difficulté technique d’acheminement à son destinataire, sera isolée ; le cas échéant supprimée.
- que l’institution peut prévoir des restrictions d’accès spécifiques à son organisation (certificats électroniques, cartes à puces ou d’authentification, filtrage d’accès sécurisé...)

L'institution informe l'utilisateur que le système d'information peut donner lieu à une surveillance et un contrôle à des fins statistiques, de traçabilité réglementaire ou fonctionnelle, d'optimisation, de sécurité ou de détection des abus, dans le respect de la législation applicable (notamment RGPD et loi informatique, fichiers et liberté).

Les personnels chargés des opérations de contrôle du système d'information sont soumis au secret professionnel.

Ils ne peuvent divulguer les informations qu'ils sont amenés à connaître dans le cadre de leurs fonctions dès lors que ces informations sont couvertes par le secret des correspondances ou qu'identifiées comme telles, elles relèvent de la vie privée de l'utilisateur.

En revanche, ils doivent communiquer ces informations si elles mettent en cause le bon fonctionnement technique des applications ou leur sécurité, ou si elles tombent dans le champ de l'article 40 alinéa 2 du code de procédure pénale.

IV. Communication électronique

1) Messagerie électronique

L'utilisation de la messagerie constitue l'un des éléments essentiels d'optimisation du travail, de mutualisation et d'échange de l' information au sein de l'institution.

La messagerie est un outil de travail ouvert à des usages professionnels administratifs, pédagogiques et de recherche : elle peut constituer le support d'une communication privée telle que définie à la section II.1).

a) Adresses électroniques

L'institution s'engage à mettre à la disposition de l'utilisateur une boîte à lettres professionnelle nominative lui permettant d'émettre et de recevoir des messages électroniques. L'utilisation de cette adresse nominative est ensuite de la responsabilité de l'utilisateur.

L'aspect nominatif de l'adresse électronique constitue le simple prolongement de l'adresse administrative il ne retire en rien le caractère professionnel de la messagerie.

L'adresse électronique nominative est attribuée à un utilisateur qui peut autoriser, à son initiative et sous sa responsabilité l'accès de tiers à sa boîte à lettres.

Une adresse électronique, fonctionnelle ou organisationnelle, peut être mise en place pour un utilisateur ou un groupe d'utilisateurs pour les besoins de l'institution.

La gestion d'adresses électroniques correspondant à des listes de diffusion institutionnelles, désignant une catégorie ou un groupe d'« utilisateurs », relève de la responsabilité exclusive de l'institution : ces listes ne peuvent être utilisées sans autorisation explicite ou validation par un modérateur.

b) Contenu des messages électroniques

Les messages électroniques permettent d'échanger principalement des informations à vocation professionnelle, liées à l'activité directe de l'institution. En toutes circonstances, l'utilisateur doit adopter un comportement responsable et respectueux des dispositions contenues dans la présente charte.

Tout message est réputé professionnel sauf s'il comporte une mention particulière et explicite indiquant son caractère privé ou s'il est stocké dans un espace privé de données.

Pour préserver le bon fonctionnement des services, des limitations peuvent être mises en place : dans ce cas, les termes en sont précisés et portés à la connaissance de l'utilisateur par le fournisseur de service de messagerie.

Sont interdits les messages comportant des contenus à caractère illicite quelle qu'en soit la nature. Il s'agit notamment des contenus contraires aux dispositions de la loi sur la liberté d'expression ou portant atteinte à la vie privée d'autrui (par exemple : atteinte à la tranquillité par les menaces, atteinte à l'honneur par la diffamation, atteinte à l'honneur par l'injure non publique, protection du droit d'auteur, protection des marques)

L'utilisation de la messagerie professionnelle par les organisations syndicales depuis le système d'information de l'institution est régie par l'accord relatif à l'usage des listes de diffusion par les organisations syndicales.

En cas de redirection des messages vers un autre serveur de messagerie, l'utilisateur doit veiller à la garantie du caractère confidentiel des messages professionnels qu'il redirige.

La redirection des messages est de la responsabilité des utilisateurs ainsi que sa mise à jour. L'institution ne connaissant et n'assurant la bonne marche que l'adresse de messagerie de l'établissement.

c) 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 les diffusions de messages en masse, l'encombrement inutile de la messagerie ainsi qu'une dégradation du service.

d) Statut et valeur juridique des messages

Les messages électroniques échangés avec des tiers peuvent, au plan juridique, peuvent constituer une preuve ou un commencement de preuve susceptible d'engager la responsabilité de l'établissement.

L'utilisateur doit, en conséquence, être vigilant sur la nature des messages électroniques qu'il échange au même titre que pour les courriers traditionnels.

e) Stockage et archivage des messages

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.

A ce titre, il doit notamment se conformer aux règles définies dans la présente charte et, le cas échéant, dans le ou les guides d'utilisation annexés.

2) Internet

Il est rappelé qu'Internet est soumis à l'ensemble des règles de droit en vigueur.

L'utilisation d'Internet (par extension intranet) constitue l'un des éléments essentiels d'optimisation du travail de mutualisation et d'accessibilité de l'information au sein et en dehors de l'institution.

L’institution met à la disposition de l’ utilisateur un accès internet chaque fois que cela est possible.

Internet est un outil de travail ouvert à des usages professionnels (administratifs et pédagogiques). Si une utilisation résiduelle privée, telle que définie en section II.1), peut être tolérée, il est rappelé que les connexions établies grâce à l’outil informatique mis à disposition par l’administration sont présumées avoir un caractère professionnel. L’administration peut les rechercher aux fins de les identifier.

L’usage des services internet ainsi que du réseau pour y accéder sont destinés à l’activité professionnelle des utilisateurs conformément à la législation en vigueur.

La mise en œuvre de services internet sur le réseau de l’établissement est soumise à un accord préalable de l’institution.

a) Publication sur les sites internet et intranet de l’institution

Toute publication de pages d’information sur les sites internet ou intranet de l’institution. Il doit être validée par un responsable de site ou responsable de publication nommément désigné.

Aucune publication de pages d’information à caractère privé (pages privées) sur les ressources du système d’information de l’institution n’est autorisée, sauf autorisation ou dispositions particulières précisées dans un guide d’utilisation établi par l’institution.

b) Sécurité

L'Institution se réserve le droit de filtrer ou d'interdire l'accès à certains sites.

Cet accès n'est autorisé qu'au travers des dispositifs de sécurité mis en place par l'institution. Des règles de sécurité spécifiques peuvent être précisées, s'il y a lieu, dans un guide d'utilisation établi par le service ou l'établissement.

L'utilisateur est informé des risques et limites inhérents à l'utilisation d'Internet par le biais d'actions de formations ou de campagnes de sensibilisation.

c) Téléchargements

Tout téléchargement de fichiers, notamment de sons ou d'images, sur Internet doit s'effectuer dans le respect, des droits de la propriété intellectuelle tels que définis à l'article VI, ou des contrats passés par l'université.

L'institution se réserve le droit de limiter le téléchargement de certains fichiers pouvant se révéler volumineux ou présenter un risque pour la sécurité des systèmes d'information (virus susceptibles d'altérer le bon fonctionnement du système d'information de l'institution, codes malveillants, programmes espions

3) Voix sur IP (VoIP) et Visioconférence

La téléphonie ainsi que les logiciels de visioconférences permettent d’échanger principalement des informations à vocation professionnelle, liées à l’activité directe de l’institution. En toutes circonstances, l’utilisateur doit adopter un comportement responsable et respectueux des dispositions contenues dans la présente charte.

Tout appel est réputé professionnel sauf s’il comporte une mention particulière et explicite indiquant son caractère privé.

Pour préserver le bon fonctionnement des services, des limitations peuvent être mises en place : dans ce cas, les termes en sont précisés et portés à la connaissance de l'utilisateur par le fournisseur de service de téléphonie.

Sont interdits les appels privés vers des plateformes impliquant un surcout à l'entreprise.
Sont également interdits les appels impliquant un contenu à caractère illicite quelle qu'en soit la nature. Il s'agit notamment des contenus contraires aux dispositions de la loi sur la liberté d'expression ou portant atteinte à la vie privée d'autrui (par exemple : atteinte à la tranquillité par les menaces, atteinte à l'honneur par la diffamation, atteinte à l'honneur par l'injure non publique, protection du droit d'auteur, protection des marques).

L'utilisation de la téléphonie professionnelle par les organisations syndicales depuis le système d'information de l'institution est régie par l'accord relatif à l'usage des listes de diffusion par les organisations syndicales.

En cas de redirection des appels vers un autre serveur de téléphonie, l'utilisateur doit veiller à la garantie du caractère confidentiel des messages professionnels qu'il redirige.
La redirection des appels est de la responsabilité des utilisateurs ainsi que sa mise à jour. L'institution ne connaissant et n'assurant la bonne marche du service de téléphonie et de visioconférence de l'établissement.

4) Unités mixtes de recherche et spécificité défense

Les unités mixtes de recherche en contrat avec l'université d'Aix-Marseille peuvent prévoir des restrictions d'accès spécifiques à leurs organisations.
Les utilisateurs de ces unités sont soumis au respect de cette charte et, quand elle existe, de la politique de sécurité du système d'information de l'unité (PSSI) édictée de l'hébergeur. Cette PSSI pourra être renforcée par celle des tutelles dont elle dépend (université, CNRS, INSERM, INRIA, …)

La transmission de données classifiées est interdite sauf dispositif spécifique agréé. La transmission de données dites sensibles doit être évitée ou effectuée sous forme chiffrée (Confidentiel défense, secret défense et très secret défense).

V. Traçabilité

L'institution est dans l'obligation légale de mettre en place un système de journalisation des accès Internet, de la messagerie et des données échangées. L'institution a également voté de la mise en place d'un système de journalisation des systèmes utiles à la mise en place du système et du réseau de l'établissement.

L'institution se réserve le droit de mettre en place des outils de traçabilité sur tous les systèmes d'information.

Préalablement à cette mise en place, l'institution procèdera, auprès de la Commission nationale de l'informatique et des libertés, à une déclaration, qui mentionnera notamment la durée de conservation des traces et durées de connexions, les conditions du droit d'accès dont disposent les utilisateurs, en application du Règlement UE 2016/679 du 27 avril 2016 et de la loi n°78-17 du 6 janvier 1978 modifiée.

VI. Respect de la propriété intellectuelle

L'institution rappelle que l'utilisation des ressources informatiques implique le respect de ses droits de propriété intellectuelle ainsi que ceux de ses partenaires et plus généralement, de tous tiers titulaires de tels droits.

En conséquence, chaque utilisateur doit :

- utiliser les logiciels dans les conditions des licences souscrites
- ne pas reproduire, copier, diffuser, modifier ou 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.

VII. Respect du RGPD et de la loi Informatique et libertés

L'utilisateur est informé de la nécessité de respecter les dispositions légales en matière de traitement automatisé de données à caractère personnel, conformément au Règlement UE 2016/679 du 27 avril 2016 dit « Règlement Général sur la Protection des Données » et à la loi n°78-17 du 6 janvier 1978 dite « Informatique et Libertés » modifiée.

Les données à caractère personnelles sont des informations qui permettent - sous quelque forme que ce soit - directement ou indirectement, l'identification des personnes physiques auxquelles elles s'appliquent.

Toutes les créations de fichiers comprenant ce type d'informations et demandes de traitement afférent, y compris lorsqu'elles résultent de croisement ou d'interconnexion de fichiers préexistants, sont soumises aux formalités préalables prévues par le Règlement UE dit « Règlement Général sur la Protection des Données » et par la loi « Informatique et Libertés ».
En conséquence, tout utilisateur souhaitant procéder à une telle création devra en informer préalablement les services compétents (et impérativement l'anciennement Correspondant Informatique et Libertés, désormais Data Privacy Officer) qui prendront les mesures nécessaires au respect des dispositions légales.

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, y compris tes données portant sur l'utilisation des systèmes d'Information.

Ce droit s'exerce auprès du responsable hiérarchique du service ou de l'établissement dont il dépend.

VIII. Limitation des usages

En cas de non-respect des règles définies dans la présente charte et des modalités définies dans les guides d'utilisation établis par le service ou l'établissement le président de l'établissement Kamen Marseille-Luminy pourra, sans préjuger des poursuites ou procédures disciplinaires ou pénales pouvant être engagées à l'encontre des personnels ou étudiants, limiter les usages par mesure conservatoire.

Le conseil d'administration de l'entreprise KameNetwork pourra, selon la gravité du préjudice et des biens engagés, engager des procédures internes et/ou judiciaires à l'encontre des personnels ou étudiants.

Tout abus dans l'utilisation des ressources mises à la disposition de l'utilisateur à des fins extra-professionnelles est passible de sanctions.

A Marseille le 10/04/2018.
Administration de KameNetwork à la date du 10/04/2018 : Paulin CARLES, Paul MOYSE, Loïc GRIMAUDO.

Charte votée par le conseil d'administration de l'Etablissement Kamen Marseille-Luminy le 10/04/2018.
Cette charte est annexée au Règlement Intérieur de l'Etablissement Kamen Marseille-Luminy.

Je soussigné, Monsieur / Madame …… , atteste avoir pris conscience de la charte informatique d'entreprise et s'engage au respect de cette dernière.

Signature (suivie de la mention « Lu et Approuvée » ainsi que de la date du jour) :