Charte régissant l'usage du système d'information de l'université d'Aix-Marseille

Sommaire

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 portables…, est 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, forum, téléphonie IP (Internet Protocol), visioconférence…

Par «institution» il faut entendre l'université d'Aix-Marseille

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 des missions du service public de l'enseignement supérieur et de la recherche;*
- *tout prestataire[3] 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[4] 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.

- Engagements de l'institution

L'institution met en œuvre les mesures nécessaires pour assurer la sécurité du système d'information et la protection des utilisateurs.

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.

- 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[5]. (Voir annexe juridique).

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

[3] Le contrat devra prévoir expressément l'obligation de respect de la charte.
[4] Ce guide juridique a été réalisé par la SDSSI.
[5] Notamment le secret médical dans le domaine de la santé.

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.

Article 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.

Article II. Conditions d'utilisation du système d'information

Section 2.1 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[6] à cet effet ou en mentionnant le caractère privé sur la ressource[7]. 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.

Section 2.2 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 l'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.

[6] Pour exemple, cet espace pourrait être dénommé "_privé_"
[7] Pour exemple, "_privé_nom_de_l_objet_" : l'objet pouvant être un message, un fichier ou toute autre ressource numérique.

Article III. Principes de sécurité

Section 3.1 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 ;
- limiter l'accès aux seules ressources pour lesquelles l'utilisateur est expressément habilité ;

✓ de la part de l'utilisateur :

- 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 l'a 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 les attaques par programmes informatiques ;
- assurer la protection de ses informations et plus particulièrement celles 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

Section 3.2 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.

Section 3.3 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 la 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[8] 40 alinéa 2 du code de procédure pénale.

[8] Obligation faite à tout fonctionnaire d'informer sans délai le procureur de la République de tout crime et délit dont il a connaissance dans l'exercice de ses fonctions.

Article IV. Communication électronique

Section 4.1 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[9] 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[10] 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

[9] L'adresse est de la forme prénom.nom@univ-amu.fr
[10] Pour exemple, les messages comportant les termes ("privé") dans l'objet ou sujet du message

(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.

Section 4.2 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[11] 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.

[11] A partir des ressources informatiques mises à la disposition de l'utilisateur

(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 …).

Section 4.3 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).**

Article V. Traçabilité

L'institution est dans l'obligation légale de mettre en place un système de journalisation[12] des accès Internet, de la messagerie et des données échangées.

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 de la loi n° 78-17 du 6 janvier 1978 modifiée.

Article 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 ;

[12] Conservation des informations techniques de connexion telles que l'heure d'accès, l'adresse IP de l'utilisateur

- 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.

Article VII. Respect 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 à la loi n° 78-17 du 6 janvier 1978 dite «Informatique et Libertés» modifiée.

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 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 la loi «Informatique et Libertés».

En conséquence, tout utilisateur souhaitant procéder à une telle création devra en informer préalablement les services compétents (et impérativement le Correspondant Informatique et Libertés) 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 les 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.

Article 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'université d'Aix-Marseille 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.

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

Le Président de l'université d'Aix-Marseille

Yvon BERLAND

Charte votée par le conseil d'administration de l'université d'Aix-Marseille le

Cette charte est annexée au Règlement Intérieur de l'Université.

Annexes

1. Annexe juridique

Sommaire

1. Préambule

La présente Annexe Juridique de l'«utilisateur» s'inscrit dans le cadre de la politique de sécurité du ministère de l'Éducation nationale (dénommé ci-après «ministère»)
L'Annexe Juridique de l'«utilisateur» est prise en application des règles édictées dans Charte régissant l'usage du système d'information par les personnels et étudiants de l'université d'Aix-Marseille, dans le prolongement de laquelle elle s'inscrit.
Elle a pour objet d'exposer à l'«utilisateur», les principales règles légales applicables, de manière non exhaustive. Ces règles en particulier ne sont pas exclusives de celles qui s'imposent à tout agent public notamment en ce qui concerne l'obligation de neutralité (religieuse, politique et commerciale), de réserve, de discrétion professionnelle et de respect des secrets protégées par la loi. Elle a une vocation pédagogique.

2. La protection des données nominatives

Les données nominatives, par exemple l'annuaire du ministère, font l'objet d'une protection légale particulière dont la violation expose son auteur à des sanctions pénales.
Les textes applicables en la matière sont les suivants :

- la loi n° 78-17 du 6 janvier 1978, modifiée par la loi n° 2004-801 du 6 août 2004, relative à l'informatique, aux fichiers et aux libertés ;
- la convention n° 108 du Conseil de l'Europe du 28 janvier 1980 pour la protection des personnes à l'égard du traitement automatisé de données à caractère personnel ;
- la directive n° 95/46 des communautés européennes du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ses données.

Ces règles s'appliquent à l'ensemble des systèmes de traitement de l'information dès lors que cette information permet d'identifier un ou plusieurs individus.
La loi du 6 janvier 1978, modifiée par la loi n° 2004-801 du 6 août 2004, a créé un dispositif juridique pour encadrer la mise en œuvre des «traitements automatisés d'informations nominatives» et ouvrir aux individus un droit d'accès et de rectification sur les données les concernant détenues et gérées par des tiers.
Cette loi impose de procéder à une déclaration et / ou une demande d'avis auprès de la CNIL préalablement à la mise en œuvre d'un traitement automatisé d'informations nominatives.
Toute personne auprès de laquelle sont collectées (oralement ou par écrit) des informations mises en œuvre dans un système automatisé de traitement doit être informée :

- du caractère obligatoire ou facultatif des réponses ;
- des conséquences d'un défaut de réponse ;
- de l'identité des destinataires des informations ;
- de l'existence d'un droit d'accès et de rectification ;

- de l'identité du responsable du traitement ;
- des finalités du traitement auquel les données sont destinées ;
- si les données sont destinées à être communiquées à des pays tiers à l'Union européenne, une information sur ce point ;
- si les données sont destinées à être utilisées à des fins de prospection, ou à être communiquées à des tiers ou utilisées pour le compte de tiers à des fins de prospection, une information sur ce point, accompagnée d'une possibilité pour les personnes de s'y opposer (au moyen d'une case à cocher ou à cliquer notamment).

3. La protection des personnes

Ainsi qu'il l'a été précédemment évoqué, les traitements automatisés d'informations nominatives sont strictement réglementés par la loi du 6 janvier 1978, modifiée par la loi n° 2004-801 du 06 août 2004.
Les dispositions relatives aux personnes sont identiques à celles décrites pour les données nominatives dans le point précédent. La violation de la loi précitée entraîne des sanctions pénales.

4. La protection des droits de propriété intellectuelle

4.1 Les règles de protection du droit d'auteur

En vertu des règles du Code de la propriété intellectuelle, l'auteur d'une œuvre de l'esprit jouit sur cette œuvre du seul fait de sa création «d'un droit de propriété incorporel et exclusif opposable à tous».
Cette disposition s'applique à toutes les œuvres de l'esprit quelqu'un soit le genre, la forme d'expression, le mérite ou la destination.
Sont notamment considérées comme des œuvres de l'esprit, au sens du Code de la propriété intellectuelle et en particulier de l'article L.112-2 les œuvres suivantes :

- les livres, brochures et autres écrits littéraires, artistiques et scientifiques ;
- les conférences, allocutions et autres œuvres de même nature ;
- les œuvres dramatiques ou dramatico-musicales ;
- les œuvres chorégraphiques ;
- les œuvres musicales avec ou sans paroles ;
- les œuvres cinématographiques et autres œuvres consistant dans des séquences animées d'images sonorisées ou non, dénommées ensembles œuvres audiovisuelles ;
- les œuvres de dessins, de peintures, d'architectures, de sculptures, de gravures, de lithographies ;
- les œuvres graphiques et typographiques ;
- les œuvres photographiques et celles réalisées à l'aide de techniques analogues à la photographie ;
- les œuvres d'art appliqué ;
- les illustrations, les cartes géographiques ;

- les logiciels, y compris le matériel de conception préparatoire.

Les actes de reproduction en tout ou partie, par tout moyen et sous toute forme sont ainsi soumis à l'autorisation du / ou des titulaire(s) des droits sur les œuvres.
L'utilisation de ces œuvres suppose donc une acceptation préalable du / ou des titulaire(s) des droits.
L'«utilisateur» est donc informé qu'à défaut d'une autorisation expresse du / ou des titulaire(s) respectant les dispositions du Code de la propriété intellectuelle, il lui est interdit d'utiliser une telle œuvre.
À défaut, sa responsabilité civile et / ou pénale peut être engagée.

4.2 Les règles de protection des logiciels

Les logiciels sont protégés par le droit d'auteur. Toute reproduction, adaptation et / ou distribution du logiciel n'est autorisée que sous réserve du consentement du titulaire des droits sur ledit logiciel.
L'étendue et les caractéristiques des droits conférés sont définies en général par des contrats de licence d'utilisation qui précisent les modalités selon lesquelles est autorisée l'utilisation des logiciels visés.
L'utilisation du logiciel, même à des fins d'essais, de démonstration de courte durée ou à des fins pédagogiques et à défaut d'autorisation expresse et écrite du titulaire des droits est en principe interdite.
L'«utilisateur» d'un logiciel s'expose à des sanctions civiles et pénales prévues et réprimées par le Code de la propriété intellectuelle lorsqu'il utilise un logiciel sans autorisation.
Afin de prévenir les risques liés à la contrefaçon de logiciel, une vigilance particulière de l'«utilisateur» comme de leur autorité hiérarchique est indispensable.
Est un délit de contrefaçon puni par le Code de la propriété intellectuelle, (article L.335-3 du Code de la propriété intellectuelle) toute reproduction, représentation ou diffusion, par quelque moyen que ce soit, d'une œuvre de l'esprit en violation des droits de l'auteur ainsi que la violation de l'un des droits de l'auteur d'un logiciel.

4.3 Les règles de protection des données

De la même façon, les données telles que les textes et, dès lors que ceux-ci présentent une certaine originalité, les images et les sons sont protégés par le droit d'auteur.
L'autorisation écrite du titulaire des droits est ainsi nécessaire pour leur utilisation. Le non-respect des dispositions relatives à la protection des droits de l'auteur sur ces données est constitutif de contrefaçon et donc soumis aux sanctions pénales prévues par la loi.
D'une manière générale, la difficulté à connaître précisément l'origine des données transmises et donc les droits y afférents, en particulier avec le développement des moyens d'échanges d'informations en réseau ouvert comme Internet, oblige l'«utilisateur» à la plus grande prudence.
4.4 Les règles de protection des bases de données
On entend par bases de données un recueil d'œuvres de données ou d'autres éléments indépendants, disposés de manière systématique ou méthodique et individuellement accessibles par des moyens électroniques ou par tout autre moyen.

Les bases de données sont protégées par le Code de la propriété intellectuelle indépendamment de la protection dont peuvent bénéficier les données au titre du droit d'auteur contenu dans ladite base.
Les bases de données qui, par le choix ou les dispositions des matières, constituent des créations intellectuelles, bénéficient des dispositions du Code de la propriété intellectuelle.
L'«utilisateur» est susceptible de se rendre coupable de contrefaçon dans plusieurs cas :

- lorsqu'il procède à toute extraction par transfert permanent ou temporaire de la totalité ou en partie, qualitativement ou quantitativement substantielle, du contenu d'une base de données sur un autre support, par tout moyen et sous toute forme que ce soit ;
- d'autre part, par la réutilisation ou par la mise à disposition de la totalité ou d'une partie qualitativement ou quantitativement substantielle du contenu de la base quelle que soit sa forme.

À ce titre, un «utilisateur» des bases de données de l'université d'Aix-Marseille ne saurait s'autoriser à utiliser à des fins privées par exemple un fichier d'adresses, dont l'université d'Aix-Marseille est propriétaire, et ne saurait le télécharger ou en faire toute utilisation contraire au Code de la propriété intellectuelle.

5. La protection des marques

Le Code de la propriété intellectuelle protège «toute marque de fabrique, de commerce ou de service servant à distinguer les produits ou services d'une personne physique ou morale» (articleL.711-1).
Peuvent être définis et utilisés à titre de marque, tous signes nominaux, figuratifs ou sonores, tels que les mots, assemblage de mots, nom patronymique, nom géographique, pseudonyme, lettre, chiffre, sigle, emblème, photographie, dessin, empreinte, logo ou la combinaison de certains d'entre eux.
Ces droits et leur protection sur une marque confèrent à son titulaire par un enregistrement un droit de propriété sur cette marque. L'«utilisateur» ne peut, sauf autorisation du propriétaire, reproduire, utiliser ou apposer une marque, ainsi qu'utiliser une marque protégée ainsi que de supprimer ou modifier une marque régulièrement déposée.
L'«utilisateur» s'interdit donc, sauf autorisation expresse du propriétaire, toute reproduction ou usage ou apposition d'une marque ainsi que l'usage d'une marque reproduite pour des produits ou services identiques à ceux désignés dans l'enregistrement, la suppression ou la modification d'une marque.
L'«utilisateur» ne saurait utiliser une marque sur laquelle l'université d'Aix-Marseille ne détient pas l'autorisation expresse d'utilisation dans le cadre de ses fonctions. Il lui sera en outre interdit d'utiliser à des fins privées toute marque dont l'université d'Aix-Marseille est titulaire.

6. La protection des Systèmes d'Information

(articles 323-1 à 323-3-1 du Code pénal)
Les atteintes aux Systèmes d'Information en tant que systèmes de traitements automatisés de données sont sanctionnées au titre de la réglementation sur la fraude informatique contenue aux articles 323-1 et suivants du Code pénal.
Ce dernier interdit notamment :

- L'accès illicite, c'est-à-dire toute introduction dans un système informatique par une personne non autorisée (article 323-1 du Code pénal). La notion d'accès s'entend de tout système de pénétration tel que la connexion pirate tant physique que logique, l'appel d'un programme alors que l'on ne dispose pas d'habilitation, l'interrogation d'un fichier sans autorisation.
- Le maintien frauduleux, c'est-à-dire le maintien sur le système informatique après un accès illicite et après avoir pris conscience du caractère «anormal» de ce maintien (article 323-3 du Code pénal). Le maintien frauduleux est notamment caractérisé par des connexions, visualisation ou opérations multiples, alors que l'accédant a pris conscience que ce maintien est «anormal».
- Le fait, sans motif légitime, d'importer, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre une ou plusieurs des infractions prévues par les articles 323-1 à 323-3 susvisés (article 323-3-1).
- L'entrave du système, c'est-à-dire toute perturbation volontaire du fonctionnement d'un système informatique (article 323-2 du Code pénal).L'entrave au système est appréhendée de manière extrêmement large car il suffit d'une influence «négative» sur le fonctionnement du système pour que le concept d'entrave soit retenu.
- L'altération des données, c'est-à-dire toute suppression, modification ou introduction de données «pirates», avec la volonté de modifier l'état du système informatique les exploitant et ce, quelle qu'en soit l'influence (article 323-1 du Code pénal). Il en est ainsi pour les bombes logiques, l'occupation de capacité mémoire, la mise en place de codification, de barrage, ou tout autre élément retardant un accès normal. Par ailleurs, la création de faux et leur usage constitue un délit autonome sanctionné au titre de faux en écriture privée, publique ou de commerce.

L'«utilisateur» doit impérativement adopter un comportement exempt de toute fraude car à défaut, il s'expose à de sévères sanctions pénales et disciplinaires

7. Le secret des correspondances

L'«utilisateur» est informé qu'est puni d'un an d'emprisonnement et de 45 000 euros d'amende «le fait, commis de mauvaise foi, d'ouvrir, de supprimer, de retarder ou de détourner des correspondances arrivées ou non à destination adressées à des tiers, ou d'en prendre frauduleusement connaissance , d'intercepter, de détourner, d'utiliser ou de divulguer des correspondances émises ou transmises par la voie de télécommunications ou de procéder à

l'installation d'appareils conçus pour réaliser de telles interceptions». (article 226-15 du Code pénal).
Il est également informé qu'est puni de trois ans d'emprisonnement et de 45 000 euros d'amende, «le fait, par une personne dépositaire de l'autorité publique ou chargée d'une mission de service public, agissant dans l'exercice ou à l'occasion de l'exercice de ses fonctions ou de sa mission, d'ordonner, de commettre ou de faciliter, hors les cas prévus par la loi, le détournement, la suppression ou l'ouverture de correspondances ou la révélation du contenu de ces correspondances…» (article 432-9 du Code pénal).

8. La responsabilité en matière de transmission des informations

Les moyens informatiques mis à la disposition de l'«utilisateur» permettent l'accès à une communication et à une information importante et mutualisée. Or, de tels moyens de communication ne doivent pas permettre de véhiculer n'importe quelle information ou donnée.
Ainsi, le Code pénal, dans ses articles 227-23 et 227-24, sanctionne le fait de fabriquer, de transporter, de diffuser, par quelque moyen que ce soit et quel que soit le support, un message à caractère violent, pornographique ou de nature à porter gravement atteinte à la dignité humaine, soit de faire commerce d'un tel message de trois ans d'emprisonnement et de 75 000 euros d'amende.
Est également puni de trois ans d'emprisonnement et de 45 000 euros d'amende, le fait de fixer, d'enregistrer ou de transmettre en vue de sa diffusion l'image d'un mineur lorsque cette dernière présente un caractère pornographique et de diffuser une telle image, par quelque moyen que ce soit.
Est puni de cinq ans d'emprisonnement et de 375 000 euros d'amende, «le fait de dissimuler, de détenir ou de transmettre une chose, ou de faire office d'intermédiaire afin de la transmettre, en sachant que cette chose provient d'un crime ou d'un délit».

9. Le respect de la vie privée

9.1 Le droit à la vie privée

Le principe est posé par l'article 9 du Code civil qui prévoit que «chacun a droit au respect de sa vie privée».
Les juges peuvent, sans préjudice de la réparation du dommage subi, prescrire toutes mesures, telles que séquestre ou autres, propres à empêcher ou à faire cesser une atteinte à l'intimité de la vie privée ;

9.2 Droit à l'image

L'«utilisateur» est informé qu'est puni d'un an d'emprisonnement et de 45 000 euros d'amende, «le fait au moyen d'un procédé quelconque, de porter volontairement atteinte à l'intimité de la vie privée d'autrui :

- 1° En captant, enregistrant ou transmettant, sans le consentement de leur auteur des paroles prononcées à titre privé ou confidentiel ;
- 2° En fixant, enregistrant ou transmettant sans le consentement de celle-ci l'image d'une personne se trouvant dans un lieu privé. Lorsque les actes mentionnés ci-

dessus ont été accomplis au vu et au su des intéressés sans qu'ils s'y soient opposés, alors qu'ils étaient en mesure de le faire, le consentement de ceux-ci est présumé» (article226-1 du Code pénal).

9.3 Le droit de représentation

L'«utilisateur» est informé qu'est puni d'un an d'emprisonnement et de 15 000 euros d'amende le fait de publier, par quelque voie que ce soit, le montage réalisé avec les paroles ou l'image d'une personne sans son consentement, s'il n'apparaît pas à l'évidence qu'il s'agit d'un montage ou s'il n'en est pas expressément fait mention (article 226-8 du Code pénal).

10. Les règles de preuve

Le principe est celui de la liberté de la preuve qui peut donc être rapportée par tout moyen. À ce titre, l'«utilisateur» est informé qu'un message électronique peut constituer une preuve susceptible d'engager la responsabilité de l4université d'Aix-Marseille ainsi que la sienne. Il est nécessaire que chaque «utilisateur» respecte scrupuleusement la législation en vigueur car le non-respect de cette obligation est passible de sanctions pénales.

2. Guide Technique Type de l’«utilisateur»

Sommaire

1. Préambule

Le présent Guide Technique Type de l'«utilisateur» a pour objet de définir les procédures techniques devant être appliquées par toute personne utilisant les moyens informatiques et de télécommunications de l'université d'Aix-Marseille.
Il complète la Charte de l'établissement régissant l'usage des technologies de l'information et de la communication en vigueur au sein de l'université d'Aix-Marseille.
Les «utilisateurs» sont informés que la violation des procédures régissant l'accès et l'utilisation des Systèmes d'Information et de télécommunications mis à leur disposition par l'université d'Aix-Marseille est susceptible d'entraîner des sanctions.

2. Champ d'application

Le présent Guide Technique Type s'applique aux «utilisateurs» et aux moyens informatiques et de télécommunication de l'université d'Aix-Marseille tels que définis dans la Charte.

3. Procédures de Sécurité

3.1 Règles de définition et de gestion des mots de passe
Chaque «utilisateur» doit veiller au respect de la sécurité liée aux mots de passe permettant l'accès à son ou ses environnements. À cet égard, chaque «utilisateur» :

- doit choisir un mot de passe sûr, n'ayant aucun lien avec l'environnement familier de l'«utilisateur» ;
- doit changer de mot de passe régulièrement, si les applications le permettent ;
- ne doit pas écrire son mot de passe sur un support facilement accessible.
- Les mots de passe choisis par les «utilisateurs» sont constitués de 6caractères alphanumériques au minimum dont au moins un chiffre et un caractère spécial.

Chaque «utilisateur» est personnellement responsable du mot de passe qu'il a choisi. À ce titre, il s'engage à :

- garder confidentiel ses mots de passe;
- changer immédiatement ses mots de passe en cas de doute sur sa confidentialité.
- En cas de perte du mot de passe ou pour la première initialisation l'utilisateur doit se présenter personnellement auprès de son correspondant sur le site.
- Ou mandater par courrier une personne de l'établissement qui se présentera auprès du correspondant du site, lequel lui remettra le mot de passe sous pli cacheté.
- Si l'utilisateur a indiqué dans l'annuaire un numéro de téléphone, il pourra à sa demande être contacté sur ce poste par le correspondant de site pour la réinitialisation du mot de passe

3.2 Paramétrage des postes de travail

Le poste de travail de l'«utilisateur» constitue un outil qui doit être protégé des intrusions. À cet égard, il convient de :

- paramétrer la mise en veille automatique des postes de travail avec demande du mot de passe pour la réactivation du poste après 15 minutes d'inactivité ;
- de ne pas se connecter au réseau ou ouvrir des sessions applicatives inutilement ;
- d'effectuer systématiquement une déconnexion des serveurs réseaux et quitter les applications actives avant de quitter son poste de travail.

4. Messagerie électronique

4.1 Messages à caractère privé

Tout message à caractère strictement privé, reçu ou émis, doit comporter en objet la mention «Privé» ou tout autre terme indiquant sans ambiguïté le caractère privé du message. Tout message ne comportant pas cette mention est réputé être un message professionnel.

L'envoi ou la réception de pièces jointes est autorisé à la condition d'être limité à un usage professionnel.

4.2 Caractéristiques et limitations de la messagerie électronique

Les messages envoyés ou reçus font l'objet d'une limitation de taille particulière. En cas de dépassement de la taille limite, le message est rejeté et l'émetteur reçoit un message de non distribution.

4.3 Stockage et archivage des messages électroniques

Chaque «utilisateur» est responsable de l'archivage et du classement des messages qu'il a relevés.

Le serveur de messagerie de l'université d'Aix-Marseille étant sauvegardé quotidiennement, les messages stockés sur le serveur sont conservés.

Chaque «utilisateur» doit en conséquence organiser lui-même la conservation des éléments en décidant :

- du nombre de génération de sauvegarde et leur périodicité ;
- du choix des fichiers et messages conservés et de ceux qui sont détruits
- du lieu et de la durée de stockage.

L'«utilisateur» doit mettre en œuvre les moyens nécessaires à la conservation des messages qui pourraient être indispensables notamment en tant qu'élément de preuve.

4.4 Sécurité anti-virale

De manière générale, il est déconseillé d'ouvrir des fichiers, de quelque nature que ce soit en provenance d'un expéditeur inconnu. En particulier, les fichiers compressés (extension en .zip par exemple) ou exécutables (extension .exe par exemple) peuvent générer l'activation de virus informatiques, code malicieux etc., susceptibles d'entraîner des conséquences d'une extrême gravité pour l'université d'Aix-Marseille.
Les «utilisateurs» sont informés que l'université d'Aix-Marseille se réserve le droit de retenir, d'isoler et / ou de supprimer tout message à l'aide de moyens automatisés et ce, sans que ces messages n'aient été nécessairement ouverts, afin de vérifier qu'ils ne comportent pas de virus.
D'une manière générale les «utilisateurs» sont informés que tout message bloquant ou présentant une difficulté technique d'acheminement à son destinataire peut être détruit sur décision de la Direction Opérationnelle des Systèmes d'Information.
Les «administrateurs» sont autorisés, en cas de difficultés majeures, à arrêter les services réseaux.

5. Web – Internet

Il est rappelé que l'accès à Internet n'est autorisé qu'au travers des dispositifs de sécurité mis en place par l'université d'Aix-Marseille.
Les «utilisateurs» ne doivent utiliser que les navigateurs sélectionnés et qualifiés par la Direction Opérationnelle des Systèmes d'Information (DOSI), dans le cadre du paramétrage et des seules extensions fournies par l'université d'Aix-Marseille.
Pour des raisons de sécurité, tout abonnement souscrit chez un prestataire de services et nécessité par l'exercice de l'activité professionnelle d'un ou de plusieurs «utilisateurs», devra faire l'objet d'une concertation préalable avec la DOSI. Il en est de même pour l'accès à des sites Web payants.

6. Matériel nomade

6.1 Les principes de précaution

Toute personne de l'université d'Aix-Marseille, à qui a été confié exclusivement dans le cadre de ses activités professionnelles un équipement de type appareil photo numérique, caméscope, téléphone portable, ordinateur portable etc., doit veiller à le protéger. En cas de non utilisation, le matériel doit être rangé dans un endroit sécurisé.
Aucun matériel non confié par l'université d'Aix-Marseille ne doit être connecté au réseau local de université d'Aix-Marseille. Par ailleurs, l'«utilisateur» doit veiller particulièrement à ne pas exposer l'équipement confié à la chaleur, à l'humidité, ni le laisser sans surveillance.

6.2 Vol

En cas de vol de l'équipement fourni, une déclaration doit être effectuée sans délai au commissariat de police le plus proche avec copie adressée à l'université d'Aix-Marseille.

6.3 Perte

En cas de perte de l'équipement confié, une déclaration détaillée doit être adressée à l'université d'Aix-Marseille.

6.4 Détérioration

En cas de détérioration du matériel portable, celui-ci doit être retourné au responsable de l'université d'Aix-Marseille accompagné du détail des circonstances dues à sa détérioration.

6.5 Sortie d'inventaire
Le vol, la perte ou la détérioration du matériel doivent être communiqués aux services de l'Agence Comptable de l'université d'Aix-Marseille pour comptabiliser la sortie du bien à l'inventaire.

7. Évolution du présent guide

Le présent Guide Technique Type de l'«utilisateur» est rédigé dans l'intérêt de chacun des «utilisateurs» et manifeste la volonté de l'université d'Aix-Marseille d'assurer un développement harmonieux et sécurisé de l'accès et de l'utilisation des moyens informatiques mis à disposition.
Le présent Guide Technique Type de l'«utilisateur» sera régulièrement mis à jour et il appartient à l'«utilisateur» de prendre connaissance de toutes nouvelles versions du Guide Technique Type qui seront portées à sa connaissance par le biais de la messagerie ou par Intranet.
Les «utilisateurs» devront veiller à se conformer aux dernières dispositions en vigueur.