Conseil d'administration
Samedi 14 octobre 2017

CHARTE REGISSANT L'USAGE DES MOYENS NUMERIQUES DE L'INSTITUT D'ETUDES POLITIQUES D'AIX EN PROVENCE

Table des matières

Article I. Champ d'application

La présente charte a pour objet de fixer les règles d'usages des moyens numériques de l'Institut d'Études Politiques d'Aix-en-Provence.

Par expression « moyens numériques », la présente charte vise tous les éléments ou toutes ressources constituant le système d'information de l'information de l'Institut d'Études Politiques d'Aix-en-Provence. Ainsi, les moyens numériques représentent l'ensemble des logiciels et matériels, outils informatiques et services numériques, que l'Institut d'Études Politiques d'Aix-en-Provence met à disposition des utilisateurs.

Les règles d'usage et de sécurité figurant dans la présente charte s'appliquent à l'Institut d'Études Politiques d'Aix-en-Provence et à l'ensemble de ses utilisateurs.

Les « utilisateurs », au sens de la présente charte, sont définis comme l'ensemble des personnes ayant obtenu l'autorisation d'accéder au système d'information de l'Institut d'Études Politiques d'Aix-en-Provence.

Les utilisateurs ayant des fonctions d'administrateurs des moyens numériques seront soumis à une charte complémentaire et spécifique précisant leurs obligations particulières.

L'ensemble de ces documents sera accessible en ligne et notamment sur le site web institutionnel de l'Institut d'Études Politiques d'Aix-en-Provence.

Article II. Conditions d'utilisation du système d'information et des moyens numériques

Section 2.1 Utilisation professionnelle / privée

L'Institut d'Études Politiques d'Aix-en-Provence met à la disposition de ses utilisateurs un ensemble d'outils et de services numériques à des fins professionnelles.

Au sens de la présente charte, l'usage des moyens numériques présente un caractère professionnel lorsqu'il intervient :

- dans le cadre des missions confiées par l'Institut d'Études Politiques d'Aix-en-Provence, pour les utilisateurs membres de son personnel : enseignants, personnels administratifs ou techniques, mais également ses prestataires et partenaires ;
- dans le cadre des activités pédagogiques, pour ses utilisateurs étudiants.

Par opposition, l'utilisation résiduelle 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 dite professionnelle à l'exception 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[1] à cet effet ou en

[1] Pour exemple, cet espace pourrait être dénommé « _privé_ »

mentionnant le caractère privé sur la ressource[2]. La ressource pouvant être un message, un fichier, ou toute autre ressource numérique. La sauvegarde régulière de 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'utilisation 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 à caractère pornographique ou illicite depuis les locaux de l'institution est interdite.

Section 2.2 Continuité de service : gestion des absences et des départs

Lors d'un départ définitif ou d'une absence ponctuelle, l'utilisateur informe sa hiérarchie des modalités d'accès aux applications et données permettant d'assurer la continuité de service.

Les mesures de conservation des données professionnelles sont définies avec le responsable hiérarchique désigné au sein de l'Institut d' Études Politiques d' Aix-en-Provence.
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 peut être engagée quant à la conservation de cet espace. Les procédures sont décrites dans le guide de l'utilisateur, annexé à la présente charte.

Article III. Principes de sécurité

Section 3.1 Règles de sécurité applicables

L'Institut d'Études Politiques d'Aix-en-Provence met en œuvre les mécanismes de protection appropriés sur les moyens numériques mis à la disposition des utilisateurs.

D'une part, l'utilisateur est informé que les codes d'accès constituent une mesure de sécurité destinée à éviter toute utilisation malveillante ou abusive. Cependant, 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 quant à lui le communiquer à son tour à un tiers, ni l'utiliser en dehors de la circonstance exceptionnelle à l'origine de sa communication.

[2] Pour exemple, « _privé_nom_de_l_objet_ » : l'objet pouvant être un message, un fichier ou toute autre ressource numérique

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

- *de la part de l'Institut d'Études Politiques d'Aix-en-Provence :*

- 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 dans le cadre de la mission de l'utilisateur. En particulier :

  L'utilisation des ressources informatiques de l'Institut d'Études Politiques d'Aix-en-Provence via la connexion d'un équipement privé et extérieur (tels qu'un ordinateur, un commutateur, un modem, une borne d'accès sans fil) sur le réseau sont interdites par défaut, sauf autorisation de l'Institut d'Études Politiques d'Aix-en-Provence.

  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 et prennent 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, qui ne proviennent pas de sites dignes de confiance, ou qui n'ont pas reçu l'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 jugées comme sensibles au sens de la politique de sécurité du système d'information (PSSI). En particulier, l'utilisateur ne doit pas transporter sans protection (telle qu'un chiffrement) des données sensibles sur des supports non fiabilisés tels que, par exemple, ordinateurs portables, clés USB ou disques externes. Les supports qualifiés comme « 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 système d'information, il convient de prendre toutes les précautions nécessaires à la non divulgation de son mot de passe et de ses données auxquelles il a accès, en cohérence avec la politique de sécurité du système d'information (PSSI).

Section 3.2 Devoirs de signalement et d'information

L'Institut d'Études Politiques d'Aix-en-Provence 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. Il signale également à la personne qui en est responsable toute possibilité soudaine 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'Institut d'Études Politiques d'Aix-en-Provence 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'Institut d'Études Politiques d'Aix-en-Provence peut prévoir des restrictions d'accès spécifiques à son organisation tels que certificats électroniques, cartes à puces ou d'authentification, filtrages d'accès sécurisé.

L'Institut d'Études Politiques d'Aix-en-Provence 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 n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et libertés).

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 identifiées comme telles. Celles-ci 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 et leur sécurité, ou si elles tombent dans le champ de l'article 40 alinéa 2 du code de procédure pénale[3].

Section 3.4 Protection antivirale

L'Institut d'Études Politiques d'Aix-en-Provence a déployé une protection logicielle généralisée non seulement sur les serveurs mais aussi sur les postes de travail des utilisateurs.

Le but d'un antivirus est de protéger toutes les machines du pars contre les attaques provoquées par des codes malveillants. Sur chaque poste utilisateur est installé un client antivirus. Il est interdit par la présente charte de désactiver, d'altérer le fonctionnement ou de désinstaller ce client. Il est aussi interdit d'utiliser d'autres logiciels (antivirus ou autres) susceptible d'entraîner un disfonctionnement de l'antivirus installé en exécution de la stratégie de sécurité de l'Institut d'Études Politiques d'Aix-en-Provence.

[3] 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'Institut d'Études Politiques d'Aix-en-Provence.

La messagerie est un outil de travail ouvert à des usages professionnels. Elle peut constituer le support d'une communication privée telle que définie à la section 2.1

(a) Adresses électroniques

L'Institut d'Études Politiques d'Aix-en-Provence 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 mais aussi pour un groupe d'utilisateurs pour les besoins de l'Institut d'Études Politiques d'Aix-en-Provence.

La gestion d'adresses électroniques fonctionnelles correspond à des listes de diffusion institutionnelles, désignant un utilisateur unique, une catégorie ou un groupe d'utilisateurs, relève de la responsabilité exclusive de l'Institut d'Études Politiques d'Aix-en-Provence : 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'Institut d'Études Politiques d'Aix-en-Provence. **L'utilisateur doit adopter en toutes circonstances 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[4] ou s'il est stocké dans un espace privé de données. Cet espace doit porter la mention « privé », « personnel » ou « assimilé ».

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 du 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 comme, par exemple, des atteintes à la tranquillité par la menace, des atteintes à l'honneur par la diffamation, des atteintes à l'honneur par l'injure non publique, la violation des droits d'auteurs, des atteintes à la protection des marques.

En cas de redirection des messages vers un autre serveur de messagerie, l'utilisateur doit veiller à garantir le 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'Institut d'Études

[4] Pour exemple, les messages comportant les termes « privé » dans l'objet ou sujet du message.

Politiques d'Aix-en-Provence ne connaissant et n'assurant le bon fonctionnement que de l'adresse de messagerie qu'elle met à disposition.

Par principe, l'adresse électronique attribuée par l'administration au personnel de l'Institut d'Études Politiques d'Aix-en-Provence prend la forme : prénom.nom@sciencespo-aix.fr

L'adresse électronique attribuée par l'administration aux étudiants de l'Institut d'Études Politiques d'Aix-en-Provence prend – sous réserve des cas d'homonymie – la forme : prénom.nom@etu-amu.fr

(c) Emission 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 et par conséquent la dégradation du service.

(d) Statut et valeur juridique des messages

Les messages électroniques échangés avec des tiers peuvent, sur le plan juridique, constituer une preuve ou un élément de preuve susceptible d'engager la responsabilité de l'institution.

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 pouvant être considérés comme éléments de preuves.

A ce titre, il doit notamment se conformer aux règles définies dans la présente charte et, le cas échéant, dans le guide de l'utilisateur, annexé à la présente charte.

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 ou Espace Membre) 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'Institut d'Études Politiques d'Aix-en-Provence.

L'Institut d'Études Politiques d'Aix-en-Provence 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 2.1 peut être tolérée, il est rappelé que les connexions établies grâce à l'outil informatique mis à disposition par l'administration sont présumés avoir un caractère professionnel. L'administration peut les rechercher aux seules 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 rigueur.

(a) Publication sur les sites Internet et Intranet / Espace Membre de l'Institut d'Études Politiques d'Aix-en-Provence

Toute publication de pages d'information sur les sites Internet et Intranet / Espace Membre de l'Institut d'Études Politiques d'Aix-en-Provence doit être validée par un responsable de service ou responsable de publication nommément désigné.

Aucune publication de pages d'information à caractère privé sur les ressources du système d'information de l'Institut d'Études Politiques d'Aix-en-Provence n'est autorisée, sauf autorisations ou dispositions particulières.

(b) Sécurité

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

L'accès général aux sites n'est autorisé qu'au travers des dispositifs mis en place par l'Institut d'Études Politiques d'Aix-en-Provence. Des règles de sécurité supplémentaires peuvent être précisées, s'il y a lieu, dans un guide d'utilisation établi par le service ou l'Institut d'Études Politiques d'Aix-en-Provence.

(c) Téléchargements

Tout téléchargement de fichiers sur Internet, notamment de sons ou d'images, doit s'effectuer dans le respect des droits de la propriété intellectuelle tels que définis à l'article VI, ou dans le cadre des contrats passés par l'Institut d'Études Politiques d'Aix-en-Provence.

L'Institut d'Études Politiques d'Aix-en-Provence se réserve le droit de limiter le téléchargement de certains fichiers pouvant se révéler volumineux ou présenter un risque pour la sécurité du système d'information tels que des virus pouvant altérer le bon fonctionnement du système d'information de l'Institut d'Études Politiques d'Aix-en-Provence, les codes malveillants ou encore les programmes espions.

Article V. Traçabilité

L'Institut d'Études Politiques d'Aix-en-Provence 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 procédera, 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, et cela en application de la loi n°78-17 du 6 janvier 1978 dite « Informatique et Libertés » modifiée.

Article VI. Respect de la propriété intellectuelle

Général

L'Institut d'Études Politiques d'Aix-en-Provence rappelle que l'utilisation des ressources informatiques implique le respect de ses droits de la propriété intellectuelle ainsi que ceux de ses partenaires et plus généralement de tous tiers titulaires de tels droits.

En conséquence, chaque utilisateur doit :

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

Anti-plagiat

Dans le cadre de sa démarche de mise en place d'outils de prévention et de détection du plagiat, l'Institut d'Études Politiques d'Aix-en-Provence met à disposition de ses enseignants chercheurs un logiciel de détection de similitude.

Ce service permet d'analyser des travaux rendus par les étudiants sous forme numérique, pour repérer et identifier les paragraphes similaires à des textes disponibles en ligne ou dans les bibliothèques de référence et dont les sources ne seraient pas citées.

> « Le plagiat consiste à :
>
> - s'attribuer les propos, les productions ou les idées d'autrui, sans citer la source ou l'auteur ;
> - s'approprier les contenus disponibles sur Internet en format textes, audio, vidéo, image, ou autre sans citer la source ou en paraphrasant de manière inadéquate. »

Sources : Université Laval, définition du plagiat. 2012, 30 mars. « Le plagiat : informer, sensibiliser et prévenir » [en ligne]. Date de consultation : septembre 2016

Légalement, le plagiat n'est pas un délit, mais la contrefaçon l'est, car on fait passer pour sien le travail d'autrui, et on le fait passer pour original.

L'Institut d'Études Politiques d'Aix-en-Provence informe ses étudiants que leurs productions (rapport de stage, mémoire, thèse, etc…) sont susceptibles d'être analysées par la solution de détection de similitudes.

Les sanctions pouvant être prises à l'encontre des responsables de plagiat sont décrites dans la charte anti-plagiat Sciences Po Aix, annexé à la présente charte.

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 le correspondant Informatique et Libertés qui sera désigné ultérieurement) 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 du système d'information. Ce droit s'exerce auprès du responsable hiérarchique du service ou de l'Institut d'Études Politiques d'Aix-en-Provence 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'Institut d'Études Politiques d'Aix-en-Provence, le directeur de l'Institut d'Études Politiques d'Aix-en-Provence pourra, sans préjuger des poursuites, 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 détaillées dans l'annexe juridique de la présente charte.

Article VIII. Limitation des usages

La présente charte sera annexée au règlement intérieur de l'Institut d'Études Politiques d'Aix-en-Provence.

La présente charte s'ajoute à tous les autres documents ou chartes relatifs à l'utilisation des moyens numériques.

Sont annexés à cette charte les documents suivants :

- annexe juridique ;
- charte anti-plagiat ;

Seront annexés à cette charte les documents suivants :

- guide d'utilisation ;
- charte des administrateurs ;

A Aix-en-Provence le

Le Directeur de l'Institut d'Études Politiques d'Aix-en-Provence

M. Rostane MEHDI

CHARTE REGISSANT L'USAGE DES MOYENS NUMERIQUES DE L'INSTITUT D'ETUDES POLITIQUES D'AIX EN PROVENCE

GUIDE DE L'UTILISATEUR

Table des matières

I- Préambule

Le présent guide pratique de l'utilisateur a pour objet d'accompagner les personnes utilisant les moyens numériques de l'Institut d'Etudes Politiques d'Aix-en-Provence dans la mise en œuvre des règles de sécurité et de comportement préconisées par la charte des bons usages.

Il est rédigé dans l'intérêt de chacun des utilisateurs et manifeste la volonté de l'Institut d'Etudes Politiques d'Aix-en-Provence d'assurer un développement harmonieux et sécurisé de l'accès et de l'utilisation des moyens numériques qu'il met à disposition.

Les utilisateurs sont informés que la violation des procédures décrites dans le présent guide peut entraîner des sanctions. La nature des sanctions encourues est précisée dans l'annexe juridique de la charte.

La charte et les documents qui la complètent, tels l'annexe juridique et le présent guide de l'utilisateur, peuvent être consultés sur le site web institutionnel à l'adresse : http://www.sciencespo-aix.fr/

Rappels :

- Quels sont les « moyens numériques » ?

Les moyens numériques de l'Institut d'Etudes Politiques d'Aix-en-Provence sont définis par l'article I al. 2 de la charte des bons usages, comme « l'ensemble des logiciels et matériels, outils informatiques et services numériques, que l'Institut d'Etudes Politiques d'Aix-en-Provence met à disposition de ses utilisateurs. ».

- Qui sont les « utilisateurs » ?

La notion d'«utilisateurs » est définie à l'article I. al. 4 de la charte comme « l'ensemble des personnes ayant obtenu l'autorisation d'accéder au système d'information de l'Institut d'Etudes Politiques d'Aix-en-Provence. ».

II- Règles de sécurité

a) Concernant la gestion des mots de passe

Chaque utilisateur doit veiller au respect de la sécurité liée aux mots de passe permettant l'accès à son environnement de travail (logiciels métiers, messagerie électronique,…)

Les mots de passe choisis par les utilisateurs devraient être constitués de 8 caractères alphanumériques au minimum, dont au moins un chiffre ou un caractère spécial. Il est vivement recommandé de changer son mot de passe, idéalement selon une périodicité de 3 mois. Chaque utilisateur est personnellement responsable du mot de passe qu'il a choisi.

Concrètement, chaque utilisateur doit :

- choisir un mot de passe sûr, n'ayant aucun lien avec son environnement familier ;
- changer de mot de passe régulièrement ;
- veiller à la confidentialité de son mot de passe et notamment s'abstenir de l'écrire sur un support facilement accessible ;
- changer immédiatement son mot de passe en cas de doute sur sa confidentialité.

b) Paramétrage des postes de travail

1- Principes généraux

Le poste de travail de l'utilisateur constitue un outil qui doit être protégé des intrusions. A cet égard il est conseillé, à chaque fois que cela sera possible :

- de paramétrer la mise en veille automatique de l'ordinateur avec demande du mot de passe pour sa réactivation après une période d'inactivité ;
- d'effectuer systématiquement une déconnexion des serveurs réseaux et de clore les applications actives avant de quitter son poste de travail.

2- Protections logicielles : anti-virus et pare feu (« firewall »)

Qu'est-ce qu'un anti-virus ?

Un anti-virus est un logiciel de protection dont le but est de détecter les virus ou logiciels malveillants. Pour cela, il inspecte la mémoire, les disques durs de l'ordinateur et les volumes amovibles (CD, DVD, clé USB, disque dur externe…) pour vérifier que les fichiers présents ne contiennent pas de codes malveillants connus. Il permet aussi d'effectuer régulièrement des analyses planifiées.

Un anti-virus protège contre les codes malveillants qu'il connaît ou qu'il reconnaît. Il est donc non seulement indispensable d'utiliser un anti-virus, mais aussi de veiller à sa mise à jour.

Qu'est-ce qu'un pare feu ?

Un pare feu ou « firewall » permet de protéger l'ordinateur connecté à Internet des attaques externes initiées par des programmes ou des personnes malveillants.

Il est indispensable de le maintenir car il représente une des principes protections actives des postes sur le réseau.

3- Mises à jour

Les logiciels, comme toute création humaine, comportent des défauts. Parmi ces défauts, on en trouve qui portent atteinte à la sécurité : ils sont appelés **« vulnérabilités »**. Au quotidien, de nombreuses vulnérabilités sont découvertes dans les systèmes d'exploitation et les logiciels équipant les matériels informatiques. Ces failles sont très rapidement exploitées par les pirates les plus expérimentés pour tenter de prendre le contrôle ou de voler des informations sur les postes de travail et les serveurs.

Il est donc primordial d'appliquer systématiquement les mises à jour de sécurité au fur et à mesure de leur publication.

4- Les périphériques de stockage

Les périphériques de stockages comme les clés USB, les disques durs externes, les cartes mémoires – voire les téléphones portables ou baladeurs qui offrent cette fonctionnalité – sont un vecteur de plus en plus utilisé pour infecter les postes de travail.

Un périphérique de stockage d'origine inconnue peut non seulement contenir des virus, mais également être configuré pour « aspirer » le contenu du poste de travail à l'insu de son propriétaire. Il est donc conseillé de :

- privilégier son propre périphérique pour un échange de données, plutôt que d'utiliser un matériel d'origine inconnue,
- d'une manière générale, il est recommandé de séparer les usages entre les périphériques de stockages professionnels et privés.

  Exemple : ne pas utiliser d'outils de type *Gmail*, *Yahoo*, *Skype* ou *Dropbox* pour des échanges professionnels. Des outils similaires sont proposés dans votre environnement numérique de travail (messagerie, échanges de fichiers…)

c) Messagerie électronique

1- Messages à caractère privé

RAPPEL : aux termes de la charte du bon usage des moyens numériques de l'IEP d'Aix-en-Provence (Art.II, Section II.1), le terme « professionnel » vise les usages n'ayant pas un caractère strictement privé. Le caractère privé n'est reconnu qu'aux actes détachés de l'exercice des missions confiées (pour les enseignants et le personnel administratif, technique de l'Institut d'Etudes Politiques d'Aix en Provence) ou détachés des activités pédagogiques (pour les utilisateurs étudiants). Les utilisateurs doivent alors :

- dans le cadre d'un message à caractère strictement privé, reçu ou émis, faire mentionner en objet la mention « Privé », afin d'exprimer sans ambiguïté le caractère extra-professionnel du message
- seront alors réputés professionnels les messages ne comportant pas, en objet, cette mention.

2- Caractéristiques et limitations de la messagerie électronique

Parmi ses fonctionnalités, la messagerie électronique permet l'échange de fichiers en « pièces jointes ». L'émission, comme la réception, de messages contenant des pièces jointes est limitée à un usage raisonnable de cette fonctionnalité. L'usage est raisonnable lorsque :

- la taille des fichiers joints, en émission ou réception, est limitée et compatible avec le bon fonctionnement du service messagerie ;
- la fonctionnalité est utilisée principalement à des fins professionnelles.

Pour prévenir les abus, les messages émis ou reçus font l'objet d'une limitation technique de non distribution. En cas de dépassement de la taille limite, le message est rejeté et l'émetteur reçoit un message de non distribution.
Par ailleurs, l'envoi de message à un grand nombre de destinataires doit être proscrit. Cette pratique provoque le ralentissement des serveurs de messagerie de l'établissement.

Surtout, les prestataires externes de services de messagerie assimilent ces messages à des « pourriels » ou « spams » et, en conséquence, placent l'université sur une liste noire. Ceci entraîne le blocage, chez les prestataires, de tous les messages en provenance de l'Institut d'Etudes Politique d'Aix-en-Provence. Pour prévenir de tels dysfonctionnements, une limite technique est mise en œuvre par la direction du Système d'Information et Stratégie Numérique : en cas d'abus, le compte de l'expéditeur est bloqué.
S'il est nécessaire de diffuser des messages à de très nombreux destinataires, il est impératif d'utiliser les listes de diffusion, qui ne provoquent aucunes perturbations.

3- Stockage et archivage des messages électroniques

L'utilisateur doit mettre en œuvre les moyens nécessaires à la conservation des messages qui pourraient être indispensables à son activité.

La messagerie des personnels de l'Institut d'Etudes Politique d'Aix-en-Provence est sauvegardée quotidiennement, ce qui ne dispense en aucun cas les utilisateurs de procéder à un archivage personnel.

Cela signifie que, malgré ce stockage sur le serveur de messagerie de l'Institut d'Etudes Politique d'Aix-en-Provence, chaque utilisateur reste responsable de l'archivage et du classement des messages qu'il a relevés.

Chaque utilisateur doit en conséquence organiser lui-même la conservation de ces éléments en décidant :

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

4- Sécurité antivirale

De manière générale, il est déconseillé d'ouvrir des fichiers en provenance d'un expéditeur inconnu. Cette prescription concerne en particulier les fichiers compressés ou exécutables dont l'ouverture peut notamment générer l'activation de virus informatique, de codes malveillants, susceptibles d'entraîner des conséquences d'une extrême gravité pour l'Institut d'Etudes Politique d'Aix-en-Provence.

Les utilisateurs sont informés que l'Institut d'Etudes Politique d'Aix-en-Provence 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 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 des Système d'Information et Stratégie Numérique.

d) Navigation sur Internet

Il est rappelé que l'accès à Internet n'est autorisé qu'au travers des dispositifs de sécurité mis en place par l'Institut d'Etudes Politique d'Aix-en-Provence.

Les utilisateurs ne doivent recourir qu'aux navigateurs sélectionnés et qualifiés par le Direction des Systèmes d'Information et Stratégie numérique (SISN), en respectant ses préconisations sur leur paramétrage et en privilégiant les extensions (plugins et modules complémentaires) recommandées par l'Institut d'Etudes Politique d'Aix-en-Provence

Certains sites malveillants profitent des failles des navigateurs récupérer les données présentes sur le poste de travail. D'autres sites mettent à disposition des logiciels qui, sous une apparence anodine, peuvent prendre le contrôle de l'ordinateur et transmettre son contenu à des tiers, à l'insu de son utilisateur.

Il convient de faire preuve de prudence, s'abstenir de se connecter à des sites suspects et éviter de télécharger des logiciels dont l'innocuité n'est pas garantie ; par exemple : vérifier la pérennité du logiciel et / ou la nature de l'éditeur.

Navigation privée
Les utilisateurs sont invités à privilégier la navigation en mode « privé », option disponible sur tous les navigateurs proposés par la SISN.

Ce mode limite le stockage des données de navigation. Il évite ainsi la conservation d'informations personnelles, dont les mots de passe, dans la mémoire du navigateur. Concrètement, il permet de supprimer les « témoins de connexion » ou « cookies », susceptibles d'engendrer des risques pour la sécurité des informations personnelles, notamment lorsque plusieurs utilisateurs ont accès au même poste.

e) Sauvegarde données : quelques repères

- L'Institut d'Etudes Politique d'Aix-en-Provence organise une sauvegarde des données sur un ensemble de postes informatiques (notamment ceux connectés au réseau « administratif »).

- Pour tous les autres, une sauvegarde régulière par chaque utilisateur est l'unique moyen de garantir la pérennité des données et de se prémunir contre les conséquences néfastes d'un problème technique, d'une attaque informatique ou d'un vol.
  La sauvegarde doit être organisée sur tout type d'appareil utilisé à titre professionnel, du poste informatique fixe au matériel nomade.

f) Matériel nomade

1- Principes généraux

Lorsqu'un équipement nomade, de type appareil photo numérique, caméscope, téléphone mobile, ordinateur portable ou tablette, est confié à un utilisateur de l'Institut d'Etudes Politique d'Aix-en-Provence, cette mise à disposition :

- est réputée intervenir dans le cadre exclusif des activités professionnelles du bénéficiaire ;
- entraine l'obligation pour le bénéficiaire d'apporter tous les soins nécessaires à la bonne conservation de ce matériel.

Par exemple, le bénéficiaire doit veiller particulièrement à :

- ne pas exposer l'équipement confié à la chaleur ni à l'humidité ;
- ne pas le laisser sans surveillance ;
- ranger le matériel non-utilisé dans un endroit sécurisé.

L'accès au réseau local est réservé au matériel confié par l'Institut d'Etudes Politiques d'Aix-en-Provence, aucun autre matériel ne doit y être connecté.

2- Vol / Perte

En cas de vol de l'équipement confié, une déclaration doit être effectuée sans délai au commissariat de police le plus proche. Une copie de cette déclaration devra être adressée à de l'Institut d'Etudes Politique d'Aix-en-Provence par l'intermédiaire du support informatique dont les coordonnées sont rappelées plus bas.

Toute fausse déclaration est passible de sanctions disciplinaires et / ou de poursuites pénales.

En cas de perte de l'équipement confié, une déclaration détaillée doit être adressée à de l'Institut d'Etudes Politique d'Aix-en-Provence par l'intermédiaire du support informatique dont les coordonnées sont rappelées plus bas.

3- Détérioration

En cas de détérioration du matériel nomade prêté, celui-ci doit être restitué au responsable de l'Institut d'Etudes Politique d'Aix-en-Provence qui a autorisé le prêt, avec un descriptif des dommages constatés et un exposé des circonstances à l'origine de la détérioration.

g) Les règles déplacement : en cas d'absences, départs ou mutations

Aux termes de l'article II.2 de la charte de bonne utilisation des moyens numériques, il appartient à tout membre du personnel, quittant à titre provisoire ou définitif l'Institut d'Etudes Politique d'Aix-en-Provence, de respecter **deux obligations** :

- permettre l'accès à ses données professionnelles en vue de garantir la continuité de service ;
- procéder à la suppression des données privées qu'il aurait stockées dans le système d'information.

1- Suppression des données privées

L'attention des agents et des enseignants de l'Institut d'Etudes Politique d'Aix-en-Provence est attirée sur la nécessité de prendre en charge personnellement la récupération puis la suppression des données privées qu'ils auraient stockées dans le système d'information de l'établissement. En conséquence, l'Institut d'Etudes Politique d'Aix-en-Provence ne peut être tenue responsable :

- de la perte des données qui n'auraient pas été récupérées par l'utilisateur avant son départ,
- de la divulgation ultérieure de données qu'il n'aurait pas supprimées.

2- Préparer son absence

Au-delà de la suppression des données privées, il convient également de :

- demander la suppression des accès aux logiciels, applications de travail (SIFAC, SOSIE, …) ;
- s'assurer de la mise en place d'un « répondeur » sur la messagerie électronique, orientant les demandeurs vers un autre contact ;
- faire retirer l'adresse électronique professionnelle des différentes listes de diffusion.

III- Pour en savoir plus

a) Liens utiles

- **ANSSI** (Agence Nationale de la Sécurité des Systèmes d'information) :*http://www.ssi.gouv.fr/*
- **Portail de la Sécurité Informatique** : *http://www.securite-informatique.gouv.fr/*
- **CERTA, Centre d'Expertise Gouvernemental de Réponse et de Traitement des Attaques informatiques** : *http://www.certa.ssi.gouv.fr/*

b) Exemples de logiciels utiles et gratuits

- **VeraCrypt** : logiciel de chiffrage pour Windows et Linux.
- **OpenVPN** : client VPN pour Windows et Linux.
- **Putty** : pour accéder à des serveurs Linux de façon sécurisée.
- **Thunderbird** : client de messagerie.
- **Firefox** : navigateur web.
- **LibreOffice** : suite bureautique compatible avec tous les systèmes.
- **Ccleaner et MalWareBytes:** nettoyeur de fichiers temporaires.

IV- Besoin d'aide ?

a) Assistance

En cas de besoin d'assistance ou de renseignements complémentaires, vous pouvez adresser vos demandes au support informatique de l'Institut d'Etudes Politiques d'Aix en Provence en écrivant à l'adresse suivante : informatique@sciencespo-aix.fr

b) Données personnelles

Le contact privilégié pour l'exercice des droits reconnus par la loi « Informatique et Libertés » et pour toutes les questions relatives à la protection des données à caractère personnel, est : informatique@sciencespo-aix.fr

Conseil d'administration
Samedi 14 octobre 2017

CHARTE REGISSANT L'USAGE DES MOYENS NUMERIQUES DE L'INSTITUT D'ETUDES POLITIQUES D'AIX EN PROVENCE

CORPUS DOCUMENTAIRE ET REGLEMENTAIRE

Table des matières

1. Préambule

La présente annexe juridique s'inscrit dans le cadre de **la politique de sécurité du ministère de l'Enseignement supérieur et de la recherche**.

Cette annexe juridique est prise en application des règles édictées dans la charte régissant l'usage du système d'information et des moyens numériques par les personnels et étudiants de l'Institut d'Etudes Politiques d'Aix-en-Provence. Elle s'inscrit dans le prolongement de celle-ci.

Elle a pour objet d'exposer à l'utilisateur les principales règles applicables de manière non exhaustive. Ces règles 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 protégés par la loi. Elle a une vocation pédagogique.

2. La protection des données nominatives et les droits des personnes concernées

a. Protection des données nominatives

Les données nominatives (l'annuaire du ministère par exemple) 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 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.
- **La loi n° 78-17 du 6 janvier 1978 modifiée**[1] relative à l'informatique, aux fichiers et aux libertés
- La loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés
- Loi n°78-735 du 17 juillet 1978 modifiée portant diverses mesures d'amélioration des relations entre l'administration et le public (CADA)
- Décret n° 2005-1309 du 20 octobre 2005 modifié pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loin° 2004-801 du 6 août 2004

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 a créé un dispositif juridique pour encadrer la mise en œuvre des «traitements automatisés d'informations nominatives» et pour 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

[1] De nombreux textes législatifs sont venus modifier la loi du 6 janvier 1978. Cette loi ainsi que la liste des textes l'ayant modifiée sont accessible à l'adresse suivante : http://www.coe.int/fr/web/conventions/full-list/-/conventions/treaty/108

procéder à une déclaration et / ou à 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 (« Droit à l'information » prévu par l'article 32 de la loi informatique et libertés) :

- 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, 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.

b. Droits des personnes concernées par des traitements de données nominatives

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. Les dispositions relatives aux personnes sont identiques à celles décrites pour les données nominatives dans le point précédent.

Il convient toutefois d'ajouter que les personnes concernées par des traitements de données disposent d'un droit d'opposition, d'accès et de rectification leur permettant de garder la maîtrise des informations qui leur sont relatives.

- Droit d'opposition (article 32 loi IL) :
  Toute personne a le droit de s'opposer, pour des motifs légitimes, au traitement de ses données, sauf si le traitement répond à une obligation légale (ex : fichiers des impôts) ou a été écarté par l'acte règlementaire autorisant la mise en œuvre du traitement (ex : APOGEE).
  Toute personne a le droit de s'opposer, sans frais et sans motif légitime, à l'utilisation de ses données à des fins de prospection commerciale : c'est le droit à la tranquillité.
- Droits d'accès et de rectification (articles 39-40 loi IL) :
  Toute personne peut, directement auprès du responsable des traitements, avoir accès à l'ensemble des informations la concernant, en obtenir la copie et exiger qu'elles soient, selon les cas, rectifiées, complétées, mises à jour ou supprimées.
  Le délai de réponse est de 2 mois.

c. Le code pénal et les atteintes aux droits de la personne résultant des fichiers ou des traitements informatiques

- **Partie législative** : Articles 226-16 à 226-24
- **Partie règlementaire** : Articles R625-10 à R625-13

3. La protection des Systèmes d'Information

Les articles 323-1 et suivants du Code pénal prévoient les sanctions (emprisonnement d'une durée variable en fonction du délit et/ou une amende) susceptibles d'être prononcées en cas d'atteintes aux Systèmes de traitements automatisés.

Parmi les atteintes, rappelées par le code pénal, à un système d'information on peut citer (liste non exhaustive) l'introduction dans un système d'information sans y être autorisée, L'entrave du système, c'est-à-dire toute perturbation volontaire du fonctionnement d'un système informatique ou encore 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.

4. 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 la transmission de messages, documents, images par quelque moyen que ce soit et quel que soit le support, à caractère violent, raciste, pornographique, terroriste, dégradant ou de nature à porter gravement atteinte à la dignité humaine est pénalement sanctionnée par des peines d'emprisonnement et d'amendes (articles 227-23 et 227-24 du Code pénal).

5. La protection des droits de propriété intellectuelle

a. Les règles de protection du droit d'auteur

En vertu des règles du **Code de la propriété intellectuelle** (CPI) :« *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* » (article L111-1 du CPI).

Cette disposition s'applique à toutes les œuvres de l'esprit quel que 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 et 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.

b. 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 son 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* », mais aussi la violation de l'un des droits de l'auteur d'un logiciel.

c. 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.

d. 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'Institut d'Etudes Politiques d'Aix-en-Provence ne saurait s'autoriser à utiliser à des fins privées par exemple un fichier d'adresses, dont l'Institut d'Etudes Politiques d'Aix-en-Provence est propriétaire, et ne saurait le télécharger ou en faire toute utilisation contraire au Code de la propriété intellectuelle.

6. La protection des marques

Le Code de la propriété intellectuelle protège la marque : « La marque de *fabrique, de commerce ou de service est un signe susceptible de représentation graphique servant à distinguer les produits ou services d'une personne physique ou morale* » (article L.711-1 du CPI).

Peuvent être définis et utilisés à titre de marque, tous signes nominaux, figuratifs ou sonores, tels que les mots, assemblages de mots, noms patronymiques, noms géographiques, pseudonymes, lettres, chiffres, sigles, emblèmes, photographies, dessins, empreintes, logos 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 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, 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'Institut d'Etudes Politiques d'Aix-en-Provence 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'Institut d'Etudes Politiques d'Aix-en-Provence est titulaire.

7. Le respect de la vie privée

a. 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 séquestres ou autres, propres à empêcher ou à faire cesser une atteinte à l'intimité de la vie privée. »

b. Le secret des correspondances

Le secret des correspondances fait partie d'un des droits de la personne ainsi les atteintes aux droits de la personne en matière de secret des correspondances sont pénalement sanctionnées par de l'emprisonnement et une amende (article 226-15 du Code pénal).

Par ailleurs la violation du secret des correspondances par des personnes exerçant une fonction publique est considérée comme une atteinte à l'administration publique également sanctionnée par une peine d'emprisonnement et une amende (article 432-9 du Code pénal).

c. Le 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 :*

- En captant, enregistrant ou transmettant, sans le consentement de leur auteur, des paroles prononcées à titre privé ou confidentiel.

- 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).

d. 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).

8. Les règles de preuve

Le principe est celui de la liberté de la preuve, liberté 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 l'Institut d'Etudes Politiques d'Aix-en-Provence, 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.