Charte d'utilisation
des ressources informatiques
de l'Université Panthéon-Assas

Le Conseil d'Administration a approuvé la Charte des utilisateurs concernant l'usage du système d'information de l'Université Panthéon-Assas en sa séance du 7 décembre 2011

INTRODUCTION

La présente charte est portée à la connaissance de tout utilisateur des ressources informatiques à l'Université Panthéon-Assas, aussi appelée « l'Université » dans ce document.

Elle définit les conditions d'accès et les règles d'utilisation des moyens informatiques et des ressources extérieures via les outils de communication de l'Université Panthéon-Assas. Elle a également pour objet de sensibiliser les utilisateurs aux risques liés à l'utilisation de ces ressources en termes d'intégrité et de confidentialité des informations traitées. Ces risques imposent le respect de certaines règles de sécurité et de bonne conduite. L'imprudence, la négligence ou la malveillance d'un utilisateur peuvent en effet avoir des conséquences graves de nature à engager sa responsabilité civile et / ou pénale ainsi que celle de l'Université.

Par *système d'information* s'entend l'ensemble des moyens matériels, logiciels, applications, bases de données et réseaux de télécommunications pouvant être mis à disposition de l'*utilisateur*.

L'informatique nomade, tel que les assistants personnels, les ordinateurs portables, les téléphones portables... est également un des éléments constitutif du système d'information.

Par *utilisateur*, s'entend toute personne ayant accès, dans le cadre de l'exercice de son activité professionnelle, aux ressources du système d'information quel que soit son statut.

Ainsi sont notamment désignés :

- Tout agent titulaire ou non titulaire, vacataire, stagiaire, hébergé, invité, doctorant, etc. ;
- Tout prestataire ayant contracté avec l'Université.

Le bon fonctionnement du système d'information suppose le respect des dispositions législatives et réglementaires qui s'imposent et notamment la sécurité, la performance des traitements et la conservation des données personnelles.

Les règles définies par la présente charte s'appliquent à l'utilisation des réseaux de l'établissement (R.E.A.G.I.R) et des réseaux extérieurs (R.E.R.I.F, R.E.N.A.T.E.R et Internet).

L'utilisation du réseau R.E.N.A.T.E.R est régie par une Charte d'Usage et de Sécurité que l'établissement, représenté par son Président, s'est engagé à respecter et à faire respecter en son sein.

Le non-respect des règles engage la responsabilité personnelle de l'utilisateur. L'établissement est lui-même soumis aux règles de bonne utilisation des moyens informatiques. À ce titre, il se doit de faire respecter lois et règles déontologiques.

PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL

La loi n°78-17 du 6 janvier 1978 modifiée en 2004 relative à l'informatique, aux fichiers et aux libertés définit les conditions dans lesquelles des traitements de données à caractère personnel peuvent être effectués. Elle ouvre aux personnes concernées par les traitements un droit d'accès et de rectification des données enregistrées sur leur compte.

L'Université a désigné un correspondant à la protection des données à caractère personnel. Ce

dernier, le CIL (Correspondant Informatique et Libertés), a pour mission de veiller au respect des dispositions de la loi n°78-17 du 6 janvier 1978 modifiée.

Il est obligatoirement consulté par le responsable des traitements préalablement à leur création.

Il recense dans un registre la liste de l'ensemble des traitements de données à caractère personnel de l'Université au fur et à mesure de leur mise en œuvre. Cette liste est tenue à disposition de toute personne en faisant la demande. Elle est également diffusée sur l'intranet de l'Université.

Le correspondant veille au respect des droits des personnes (droit d'accès, de rectification et d'opposition). En cas de difficultés rencontrées lors de l'exercice de ces droits, les personnes concernées peuvent saisir le correspondant (coordonnées en annexe).

ENGAGEMENTS

Engagements de l'Université Panthéon-Assas

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

L'Université facilite l'accès des utilisateurs aux ressources du système d'information. Les ressources mises à leur disposition sont prioritairement à usage professionnel mais l'Université est tenue de respecter la vie privée de chacun.

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

Ils ont accès à l'ensemble des données techniques mais s'engagent à respecter les règles de confidentialité applicables aux contenus des documents.

Ils sont assujettis au devoir de réserve et sont tenus de préserver la confidentialité des données qu'ils sont amenés à connaître dans le cadre de leurs fonctions.

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.

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

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

CHAMP D'APPLICATION DE LA CHARTE

Les règles d'usage et de sécurité figurant dans la présente charte s'appliquent à l'Université Panthéon-Assas ainsi qu'à l'ensemble de ses utilisateurs.

La charte est diffusée à l'ensemble des utilisateurs par note de service et, à ce titre, mise à disposition sur la page d'accueil de l'ENT de l'Université. Elle est systématiquement remise à tout nouvel arrivant.

I - Conditions d'utilisation des systèmes d'information

I.1 *Utilisation professionnelle / privée*

Les communications électroniques (utilisation des ressources informatiques, usage des services internet, usage du réseau) sont destinées à l'activité professionnelle des utilisateurs. L'activité professionnelle doit être entendue comme celle définie par les textes spécifiant les missions du service public de l'enseignement supérieur.

Elles peuvent cependant constituer le support d'une communication privée. L'utilisation résiduelle du système d'information à titre privé doit être non lucrative et raisonnable, tant dans la fréquence que dans la durée. Elle ne doit pas nuire à la qualité du travail de l'utilisateur, au temps qu'il y consacre et au bon fonctionnement du service.

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

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

I.2 *Continuité de service : gestion des absences et des départs*

Aux seules fins d'assurer cette continuité, l'utilisateur devra utiliser, pour les activités liées à sa fonction, et dans la mesure du possible, une adresse de fonction et les espaces partagés mis à sa disposition.

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. Dans le cas où cet espace de données à caractère privé n'aurait pas été détruit par l'utilisateur, l'Université s'engage à ne divulguer aucun des éléments y figurant à des tiers, sauf cas prévus par la réglementation.

L'utilisateur pourra demander à accéder à son compte mail pendant une durée de trois mois après son départ définitif. Au-delà, les données de cet espace seront détruites.

L'utilisateur doit garantir l'accès à tout moment à ses données professionnelles. En cas d'absence non planifiée et pour des raisons exceptionnelles, si un utilisateur se trouve dans l'obligation de communiquer ses codes d'accès au système d'information, il doit procéder dès que possible aux changements de ses derniers ou en demander la modification à l'administrateur.

I.3 *Utilisation conforme aux lois en vigueur*

(a) *Respect de la propriété intellectuelle*

L'Université rappelle que l'utilisation des moyens informatiques implique le respect de ses droits de propriété intellectuelle ainsi que ceux de ses partenaires et plus généralement, de tout tiers titulaires de tels droits. En conséquence, chaque utilisateur doit :

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

(b) *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 par la loi n° 2004-801 du 6 août 2004.

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 traitements comprenant ce type d'informations, y compris lorsqu'elles résultent de croisement ou d'interconnexion de traitements préexistants, sont soumises aux

formalités préalables prévues par la loi Informatique et Libertés.

En conséquence, tout utilisateur souhaitant procéder à un tel traitement devra le déclarer auprès du Correspondant Informatique et Libertés (CIL) de l'Université.

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 du traitement.

(c) *Respect de la vie privée*

Le droit à la vie privée, le droit à l'image et le droit de représentation implique qu'aucune image ou information relative à la vie privée d'autrui ne doit être mise en ligne sans un consentement de la personne intéressée.

(d) *Respect des clauses contractuelles*

Les ressources documentaires électroniques éditoriales dans les conditions contractuelles des licences souscrites par l'Université : usage raisonnable (pas de téléchargement de livres complets ou de fascicules entiers de revues, pas d'utilisation d'aspirateur de site Web), usage personnel et strictement non commercial (interdiction de distribuer des copies papier ou de diffuser des versions numériques à toute personne extérieure à l'Université, même à titre gratuit).

(e) *Responsabilités en matière de transmission d'informations*

L'utilisateur devra entre autres s'abstenir :

- de diffuser des messages diffamatoires ou injurieux (ces faits sont répréhensibles quel que soit leur mode de diffusion, public ou privé) ;
- d'utiliser certaines formes d'apologie (crime, racisme, négationnisme, crimes de guerre, etc.) ;
- d'utiliser toute forme de provocation et de haine raciale ;
- de diffuser des informations confidentielles sans autorisation préalable d'une personne habilitée.

II. Principes de sécurité

II.1 *Règles de sécurité applicables*

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

En particulier tout utilisateur du système d'information de l'Université doit être référencé dans les bases de l'Université et avoir obtenu un *sésame*, c'est-à-dire les codes d'accès « authentifiant et mot de passe », qui lui sont personnels et confidentiels.

L'utilisateur est informé que les codes d'accès constituent une mesure de sécurité permettant de protéger les données et les outils auxquels il a accès de toute utilisation malveillante ou abusive. Cette mesure ne confère pas pour autant un caractère personnel à ces données ou outils.

Les niveaux d'accès ouverts à l'utilisateur sont définis en fonction de la mission qui lui est conférée. La sécurité des systèmes d'information mis à sa disposition lui impose :

- de respecter les consignes de sécurité, notamment les règles relatives à la gestion des mots de passe ;
- de garder strictement confidentiel(s) son (ou ses) mot(s) de passe et ne pas le(s) dévoiler à un tiers ;
- de protéger son certificat électronique (s'il en dispose) par un mot de passe sûr gardé secret.

Comme la signature manuscrite, le certificat électronique est strictement personnel et

l'utilisateur s'engage à n'autoriser personne à en faire usage à sa place.

Si pour des raisons exceptionnelles et ponctuelles, un utilisateur se trouve dans l'obligation de communiquer son mot de passe, il devrait 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 qui lui a fait bénéficier de ce mot de passe.

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

(a) *de la part de l'Université* :

- 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 (cf. I.2) ;
- limiter l'accès aux seules ressources pour lesquelles l'utilisateur est expressément habilité ;
- ne pas autoriser les redirections de messagerie pour les adresses de fonction dans la mesure où le système d'information est accessible (après authentification) tant du réseau de l'Université que de l'extérieur.

(b) *de la part de l'utilisateur* :

- s'interdire d'accéder ou de tenter d'accéder à des ressources du système d'information et aux communications entre tiers pour lesquelles il n'a pas reçu d'habilitation explicite ;
- ne pas utiliser les services qui lui sont offerts pour proposer ou rendre accessibles à des tiers des données et informations confidentielles ou contraires à la législation en vigueur ;
- ne pas connecter directement aux réseaux locaux des matériels autres que ceux confiés ou autorisés par l'Université, ou ceux dont la liste a été précisée dans un guide d'utilisation établi par le service ou par l'établissement. 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 connecté au réseau de l'Université, 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 sa hiérarchie ;
- ne pas déposer des données sur un serveur interne ou ouvert au grand public (Google, Free, Orange, …) ou sur le poste de travail d’un autre utilisateur sans y être autorisé par les responsables habilités ;
- ne pas apporter volontairement des perturbations au bon fonctionnement des ressources informatiques et des réseaux que ce soit par des manipulations anormales du matériel, ou par l’introduction de logiciels parasites (virus, chevaux de Troie, bombes logiques...). Tout travail de recherche ou autre, risquant de conduire à la violation de cette règle, ne pourra être accompli qu’avec l’autorisation du Responsable de la Sécurité du Système d'Information de l'Université et dans le strict respect des règles qui auront alors été définies ;
- 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, y compris en utilisant différents moyens de sauvegarde individuels ou mis à sa disposition. En particulier, il ne doit pas transporter sans protection (telle qu’un chiffrement) des données sensibles sur des supports non fiables tels que ordinateurs portables, clés USB, disques externes, etc ;
- ne pas quitter son poste de travail ni ceux en libre-service en laissant des ressources ou services accessibles.

En outre, il convient de rappeler que les visiteurs ne peuvent avoir accès au Système d'Information de l'Université sans l'accord préalable du service informatique interne.

Les intervenants extérieurs doivent s'engager à faire respecter la présente charte par leurs propres salariés et éventuelles entreprises sous-traitantes. Dès lors, les contrats signés entre l'Université Panthéon-Assas et tout tiers ayant accès aux données, aux programmes informatiques ou autres moyens, doivent comporter une clause rappelant cette obligation.

II.2 *Devoirs de signalement et d'information*

L'Université 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 au Responsable de la sécurité des systèmes d'information (RSSI) toute possibilité d'accès à une ressource qui ne corresponde pas à son habilitation (coordonnées en annexe).

II.3 *Mesures de contrôle de la sécurité*

L'utilisateur est informé :

- que pour effectuer la maintenance corrective, curative ou évolutive, l'Université 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 ou présentant une difficulté technique d'acheminement à son destinataire peut être isolée, le cas échéant supprimée.

L'Université informe l'utilisateur que le système d'information peut donner lieu à une surveillance et un contrôle à des fins statistiques, de traçabilité, d'optimisation, de sécurité ou de détection des abus.
Les personnels en charge des opérations de contrôle sont soumis au secret professionnel. Ils ne peuvent donc pas divulguer les informations qu'ils sont amenés à connaître dans le cadre de leur fonction 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 ;
- elles ne mettent en cause ni le bon fonctionnement technique des applications, ni leur sécurité ;
- elles ne tombent pas dans le champ de l'article 40 alinéa 2 du code de procédure pénale qui fait obligation à tout organe public de déférer des faits délictueux au procureur de la République.

III. Communications électroniques

III.1 *Messagerie électronique*

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

La messagerie est un outil de travail ouvert à des usages professionnels (administration, pédagogie, recherche) ; elle peut constituer le support d'une communication privée telle que définie à l'article II. A cette fin, l'Université recommande l'utilisation d'adresses de messagerie privée.

(a) *Adresses électroniques*

L'adresse électronique nominative est attribuée à un utilisateur qui la gère sous sa responsabilité. L'utilisation d'une adresse électronique, fonctionnelle ou organisationnelle, est fortement conseillée pour un utilisateur ou un groupe d'utilisateurs.

(b) *Contenu des messages électroniques*

Pour préserver le bon fonctionnement des services, des limitations peuvent être mises en place : dans ce cas, les termes en sont précisés dans un guide d'utilisation de la messagerie qui est porté à la connaissance des utilisateurs.

Tout message est réputé professionnel sauf s'il comporte une mention particulière et explicite indiquant son caractère privé. Dans ce cas et afin de lui conserver son caractère privé, l'utilisateur doit le déposer dans un dossier identifiable comme « personnel ».

(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, former un contrat, sous réserve du respect des conditions fixées par les articles 1369.1 à 1369.11 du code civil.

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 utiles en tant qu'éléments de preuve.

À ce titre, il doit notamment se conformer aux règles définies dans la présente charte et, le cas échéant, dans le ou les guide(s) d'utilisation établi(s) par le service ou par l'établissement.

III.2 *Internet*

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

(a) *Publications sur les sites Internet et Intranet de l'Université*

Toute publication de pages d'informations ou de documents sur les sites Internet ou Intranet de l'institution doit être validée par un responsable de site ou responsable de publication nommément désigné.

Aucune publication de pages d'information (ou documents) à caractère privé sur les ressources du système d'information de l'institution n'est autorisée, sauf disposition particulière précisée dans un guide d'utilisation établi par le service ou par l'établissement.

Il est à noter que les pages, dites personnelles professionnelles :

- sont des pages Web du domaine « u-paris2.fr » (ou d'un de ses sous-domaines) placées sous la responsabilité d'un personnel de l'Université, d'une association, d'un groupement ; elles doivent être fiables et l'on doit pouvoir facilement les dater, identifier leur producteur et comprendre à quel titre il les rend accessibles ;
- contiennent des informations de nature professionnelle, en rapport avec le métier du responsable ou avec les missions de l'Université ce qui implique une responsabilité sur le contenu informatif (exactitude, légalité, pertinence, ...), leur pérennité et leur intégrité.
- concourent comme les autres à l'image de l'Université et des autres tutelles dans le cas des unités mixtes de recherche; il est donc interdit d'engager l'Université et les autres tutelles ou de nuire à leur réputation ou à celle de l'un de leurs membres.

(b) *Sécurité*

L'Université se réserve le droit de filtrer ou d'interdire l'accès à certains sites, de procéder au contrôle a priori ou a posteriori des sites visités et des durées d'accès correspondantes.

Cet accès n'est autorisé qu'au travers des dispositifs de sécurité mis en place par l'Université. 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 le réseau Internet doit s'effectuer dans le respect des droits de la propriété intellectuelle tels que définis à l'article I.3 L'Université 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'Université, code malicieux, programmes espions ...).

À l'inverse, l'utilisation du réseau pour l'offre d'un service disponible depuis l'Internet doit être rationnelle de manière à éviter toute consommation abusive ; notamment toute mise en service d'un serveur doit être déclarée, ne serait-ce que pour en autoriser l'accès depuis l'extérieur du réseau de l'Université. L'offre de sons, d'images, de vidéos, de logiciels et tous autres documents doit s'effectuer dans le respect des droits de la propriété intellectuelle tels que définis dans la section I.3 et être en rapport avec les missions d'enseignement et de recherche de l'Université.

III.3 *Unités mixtes de recherche et spécificité Défense*

Dans le cas d'une UMR, celle-ci peut prévoir des restrictions d'accès spécifiques à son organisation.

Les utilisateurs de ces unités sont notamment soumis au respect, quand elles existent, des Politiques de Sécurité du Système d'Information de l'unité (PSSI) édictées par les tutelles correspondantes (Université, CNRS, Inserm, Inria, ...).

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

IV. Traçabilité

L'Université est dans l'obligation légale de mettre en place un système de journalisation des accès Internet, de la messagerie et des données échangées. L'Université a mis en place des outils de traçabilité sur tous les systèmes d'information.

Un document décrivant la politique de gestion des journaux informatiques (et mentionnant notamment la durée de conservation des traces) a été enregistré dans le registre tenu par le Correspondant Informatique et Libertés de l'Université, en application de la loi N° 7817 du 6 janvier 1978 modifiée par la loi N° 2004-801 du 8 août 2004.

V. Limitation des usages

En cas de non-respect des règles définies dans la présente charte et des modalités définies dans les guides d'utilisation, le *Président de l'Université* pourra, sans préjuger des poursuites ou procédures de sanctions pouvant être engagées à l'encontre des personnels, limiter les usages par mesure conservatoire.

Tout abus dans l'utilisation des ressources mises à la disposition de l'utilisateur à des fins extraprofessionnelles, est passible de sanctions.

VI. Entrée en vigueur de la charte

La présente charte sera annexée au règlement intérieur de l'Université Panthéon-Assas, dès sa création.

ANNEXES

I. Dispositions légales applicables

Directive 95/46/CE 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 ces données.

Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée par la loi n°2004-801 du 6 août 2004.

Dispositions Pénales :

Code Pénal (partie législative) : art 226-16 à 226-24

Code Pénal (partie réglementaire) : art R. 625-10 à R. 625-13

Loi n°88-19 du 5 janvier 1988 relative à la fraude informatique dite loi Godfrain.

Dispositions Pénales : art 323-1 à 323-3 du Code Pénal.

Loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (LCEN)

Loi n°94-361 du 10 mai 1994 sur la propriété intellectuelle des logiciels.

Disposition Pénale : art L.335-2 du Code Pénal.

II. Administrateurs du système d'information

La présente annexe a pour objet de formaliser les règles de déontologie et de sécurité s'appliquant spécifiquement aux administrateurs du système d'information de l'Université.

Cette annexe est indissociable de la charte informatique du système d'information de l'Université qu'elle complète en précisant les droits et devoirs des administrateurs du système d'information.

1. *Définition et mission d'un administrateur du système d'information*

Le terme « administrateur » désigne toute personne, employée ou non par l'Université, chargée explicitement du bon fonctionnement et de la sécurité de ressources informatiques faisant partie du système d'information de l'établissement et qui sont placées sous sa responsabilité.

Dans le but d'assurer la disponibilité, l'intégrité, la confidentialité et la journalisation des accès aux données, réseaux, systèmes et applications dont il a la responsabilité, l'administrateur met en œuvre les mesures SSI (Sécurité du Système d'Information) nécessaires. Ces mesures doivent respecter la législation en vigueur, la PSSI d'établissement et la PSSI de l'entité le cas échéant. Elles doivent inclure les mesures émanant du Haut fonctionnaire de Défense et de Sécurité du ministère de tutelle et celles préconisées par le RSSI dans le but de couvrir un risque SSI clairement identifié. Leur mise en place est conditionnée par la définition des objectifs de sécurité fixés par la direction de l'entité, juridiquement responsable en cas d'incident, et par les moyens pouvant y être affectés.

2. *L'administrateur et la sécurité du système d'information*

Dans le cadre de l'exploitation, la maintenance et le suivi de l'utilisation des ressources informatiques de son périmètre d'activité, l'administrateur du système d'information est amené à effectuer des actions spécifiques lui permettant d'assurer la continuité de service. Ces actions lui donnent potentiellement accès à l'ensemble des données utilisateurs. Habituellement, les données auxquelles il accède se limitent aux données issues de la métrologie, de la surveillance, de l'audit des réseaux et systèmes et/ou aux données nécessaires aux diagnostics de dysfonctionnements et aux recherches de malveillances. En cas d'incident, des investigations peuvent cependant l'amener à prendre indirectement connaissance d'informations de nature confidentielle, si ces données ne sont pas protégées par un mécanisme de chiffrement ; il est alors soumis au devoir de confidentialité.

Les équipements, systèmes, applications, ainsi que les outils dont l'administrateur fait usage dans l'exercice de sa fonction, sont exclusivement professionnels et autorisés par l'Université. Aucun système, logiciel ou progiciel ne peut être installé sans qu'une licence d'utilisation n'ait été préalablement souscrite.

L'administrateur met en œuvre une procédure de gestion des accès aux ressources informatiques ainsi que des mécanismes d'authentification conformes à la PSSI.

Une trace écrite (date et heure, description des événements, solution mise en œuvre, etc.) de tous les incidents de sécurité survenus dans son périmètre d'activité doit être conservée.

Enfin, l'administrateur est responsable de la mise à jour des systèmes, applications et dispositifs de sécurité, (nouvelles versions, correctifs de sécurité, etc.) dont il a la charge. Ces mises à jour doivent être effectuées avec discernement : maturité de la dernière version, accord éventuel des éditeurs des logiciels hébergés, non-régression des services, etc. sont à prendre en compte avant tout changement majeur. Il est chargé de la documentation des procédures qu'il met en place pour l'administration des services vitaux.

3. *Droits et devoirs spécifiques*

L'administrateur est soumis à la présente charte informatique. Il doit, d'une manière générale, respecter les règles d'éthique professionnelle et de déontologie, l'obligation de réserve ainsi que le devoir de discrétion.

Cependant, pour exercer son rôle au sein du système d'information de l'établissement, il a des droits et des devoirs spécifiques.

Dans le cadre de ses missions, l'administrateur a le droit :

- d'être informé des implications légales de son travail, y compris des risques qu'il encourt dans le cas où un utilisateur du système dont il a la charge commettrait une action répréhensible ;
- de prendre toute disposition nécessaire au bon fonctionnement des ressources informatiques dont il a la charge ;
- d'établir des procédures de surveillance des données, réseaux, systèmes et applications, afin de déceler les anomalies, en accord avec la PSSI et en ayant préalablement informé les utilisateurs ;
- d'accéder à toute information utile (y compris les fichiers de journalisation) à des fins de diagnostic et d'administration du système, en respectant ses engagements de confidentialité et de non-divulgation de ces informations.

Dans le cadre de ses missions, l'administrateur a le devoir :

- d'améliorer en permanence la qualité de service et de la sécurité, dans l'intérêt de l'entité, de l'établissement et des utilisateurs ;
- de respecter la plus stricte confidentialité des mots de passe des utilisateurs dont il aurait pu avoir connaissance ;
- de garder strictement confidentiel son mot de passe administrateur sous réserve des nécessités de continuité de service ;
- Pour des raisons de continuité de service (ceci est une obligation pour les services vitaux), il est fortement recommandé que l'administrateur communique (ou donne accès à une procédure de recouvrement) les mots de passe liés à son activité à au moins un autre personnel de l'entité (autre administrateur des ressources informatiques, RSSI, responsable hiérarchique…) susceptible d'intervenir en son absence pour la pérennité de la ressource. Le bénéficiaire n'est pas autorisé à accéder aux répertoires, données et messages dont le caractère privé est explicite.
- Pour son activité de veille technologique, l'administrateur dispose de la diffusion d'informations par les fabricants de matériels, les éditeurs de logiciels et autres sources spécialisées, des avis et recommandation des CERT (relayés par le RSSI), de sites dédiés tels que www.securite-informatique.gouv.fr ou www.cnil.fr (ex : http://www.cnil.fr/la-cnil/actu-cnil/article/article/10-conseils-pour-securiser-votre-systeme-dinformation/), etc.
- de respecter la confidentialité absolue des informations privées ou à caractère personnel dont il a eu connaissance dans le cadre de l'exercice de sa mission, ces informations ne pouvant légalement être communiquées qu'aux personnes appartenant à la chaîne fonctionnelle de sécurité du système d'information de l'Université et aux autorités judiciaires ;
- de veiller à ce que les tiers non-autorisés n'aient pas connaissance d'informations privées ou à caractère personnel ;
- d'organiser la continuité des services numériques (équipements, documentation, accès…) afin de minimiser les conséquences de son éventuelle indisponibilité ;
- de mettre en œuvre un système de journalisation des accès aux ressources informatiques (logs) conforme à la Politique de Gestion des Journaux Informatiques de l'Université ;
- d'examiner régulièrement ces journaux pour une détection précoce des dysfonctionnements et incidents de sécurité ;
- de veiller à la déclaration des traitements automatisés d'informations nominatives, conformément à la réglementation en vigueur ;
- de refuser de répondre à une demande qui aurait pour conséquence de lui faire commettre une infraction (droit à la vie privée, droit au secret de la correspondance,

loi Informatique et Libertés, etc…), en dehors des requêtes des autorités judiciaires ;

- d'agir au plus tôt lorsqu'il a connaissance d'action illégales ou de données illicites sur les équipements, systèmes ou applications dont il a la responsabilité en isolant le composant en cause (fichier, serveur…), et en informant le RSSI ;
- de veiller au respect, par les utilisateurs, de la présente Charte Informatique et des consignes de sécurité figurant dans la PSSI.
- L'administrateur doit tenir informée la direction de son entité des choix et difficultés techniques liés à l'exercice de sa fonction : propositions d'amélioration des services et de la sécurité, conseil en ingénierie informatique, budget en accord avec les objectifs, besoins de formations, etc.
- L'administrateur doit tenir informé le RSSI des incidents de sécurité et vulnérabilités du système d'information rencontrés dans l'exercice de sa mission : tentatives d'intrusion, virus détectés, matériels obsolètes, saturation de ressources informatiques, plan de reprise/continuité d'activité non opérationnel, etc… D'une manière générale, il doit signaler tout événement, règle de sécurité violée, charte informatique non respectée, et toutes autres activités non conformes à la PSSI pouvant avoir un impact légal ou réglementaire ou bien induisant un risque (technique, juridique, financier, image de marque…) non négligeable pour l'entité.

4. *Chaîne d'alerte de l'Université*

L'administrateur doit mettre en œuvre les mesures issues de la chaîne d'alerte de la sécurité informatique de l'établissement. En particulier, il lui incombe de :

- prendre toutes mesures nécessaires suite aux alertes des CERT et aux consignes de la chaîne fonctionnelle de sécurité du système d'information de l'Université lorsque les ressources informatiques dont il a la responsabilité sont concernées ;
- fournir au RSSI les informations nécessaires à l'évaluation de la gravité d'un incident de sécurité et, le cas échéant, apporter les éléments nécessaires à la constitution du dossier pour suite à donner ;
- coopérer à la résolution des incidents et se conformer aux directives de la PSSI, aux demandes des CERT et aux consignes du RSSI, en fonction de la nature et de la gravité de l'incident ;
- répondre aux sollicitations des autorités judiciaires (généralement relayées par un Officier de Police Judiciaire) en relation avec la chaîne fonctionnelle de sécurité du système d'information de l'établissement.

5. *Information des utilisateurs*

La mise à disposition de ressources informatiques s'accompagne nécessairement d'une information auprès des utilisateurs concernés. L'administrateur est donc tenu de :

- porter à leur connaissance les informations et les traitements auxquels il a accès de par sa fonction ;
- les informer, dans la mesure du possible, de toute intervention nécessaire, susceptible de perturber ou d'interrompre l'utilisation habituelle des ressources informatiques ;
- les informer des derniers incidents ayant perturbé ou interrompu l'utilisation habituelle des ressources informatiques ;
- les informer de toute opération conduisant à accéder à leur poste informatique, et du motif justifiant cette intervention (sauf lorsque la discrétion des opérations est imposée par les autorités judiciaires) ;
- leur communiquer les règles de bon usage du système d'information de l'Université et du réseau RENATER, les sensibiliser aux problèmes de sécurité informatique, leur faire connaître les consignes techniques de sécurité, en appui des actions du RSSI.

6. *Mesures conservatoires*

Le non-respect, délibéré et en connaissance de cause, par un administrateur des règles spécifiques définies dans la présente annexe peut entraîner des sanctions de natures disciplinaires et/ou pénales.

III. Quelques références

Serveur institutionnel de l'établissement :

http://www.u-paris2.fr

Serveur intranet de l'établissement :

https://intranet.u-paris2.fr

Adresse du responsable de la sécurité du système d'information (RSSI) :

rssi@u-paris2.fr

Adresse du correspondant informatique et libertés (CIL) :

cil@u-paris2.fr

Pages intranet Informatique et libertés :

https://intranet.u-paris2.fr/Generalites/CNIL/cnil.html

Ces références peuvent être modifiées ; la version en ligne de ce document sera maintenue à jour.

IV. Glossaire

Ci-dessous l'explicitation de sigles et termes employés dans le document :

Antispams : logiciels conçus pour détecter et éliminer les spams. Basés sur diverses méthodes de reconnaissance (analyse de l'entête, analyse du contenu, réputation et/ou comportement du relais de messagerie, etc…), ils sont mis en œuvre sur les passerelles de messagerie et/ou les postes de travail.

Antivirus : logiciels conçus pour détecter et éliminer des codes malveillants tels que virus, vers, chevaux de Troie. Basés sur une recherche de signatures (partie de code spécifique), ils sont mis en œuvre sur les passerelles de messagerie et/ou les postes de travail.

Bombe logique : logiciel destiné à altérer ou détruire partiellement ou totalement un système informatique (déclenchement sur date ou autre événement).

Canular informatique (Hoax en anglais) : forme de spam dont la diffusion se fait de proche en proche (chaîne de lettres par exemple). La forme de propagation (destinataire sollicité pour faire suivre vers ses correspondants habituels, contenu alarmant mais plausible…) endort la vigilance des destinataires et rend sa détection difficile par les antispams.

Cheval de Troie (Trojan horse en anglais) : code malveillant généralement intégré à un programme légitime pour effectuer une action nuisible. Beaucoup comportent une porte dérobée (backdoor en anglais) permettant une prise de contrôle à distance de l'ordinateur.

CIL (Correspondant Informatique et Libertés) : le CIL veille à la bonne application de la loi informatique et libertés dans l'établissement ; il doit établir et maintenir un registre des traitements mis en œuvre dans l'établissement.

CNIL (Commission Nationale de l'Informatique et des Libertés) : autorité administrative indépendante créée par la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

DSI (Direction du Système d'Information) : service en charge du système d'information de l'Université (ensemble de services numériques mis à la disposition des communautés enseignement, recherche et administration de l'établissement). Il en assure l'exploitation au quotidien et son évolution dans le cadre du schéma directeur du système d'information.

Hameçonnage (Phishing en anglais) : sollicitation frauduleuse d'extorsion de mot de passe (ou autre information personnelle sensible telle que numéro de Carte Bleue) par messagerie ou via un site web contrefait.

Journaux informatiques (traces ou logs) : données de connexion pouvant aider à retracer les attaques, les activités inhabituelles ou inappropriées qu'elles soient d'origine interne ou externe.

Malware (code malveillant en français) : mot générique pour désigner un logiciel nuisible pour le système d'information (virus, ver, cheval de Troie, porte dérobée, logiciel espion, etc…).

PGJI (Politique de gestion des Journaux Informatiques) : ensemble de règles encadrant la collecte, les traitements et les destinataires des informations à caractère personnel recueillies par les systèmes informatiques lors de leur accès par les utilisateurs.

PSSI (Politique de Sécurité du Système d'Information) : ensemble formalisé dans un document applicable, des directives, procédures, codes de conduite, règles organisationnelles et techniques, ayant pour objectif la protection du système d'information de l'établissement.

RAP (Réseau Académique Parisien) : assure l'interconnexion de l'ensemble des sites enseignement supérieur et recherche parisiens ainsi que leur connexion Internet via RENATER.

RENATER (Réseau National de télécommunications pour la Technologie l'Enseignement et la Recherche) : interconnecte les établissements, directement ou via des réseaux de collecte type RAP, ayant une activité dans les domaines de la recherche, la technologie et l'enseignement. RENATER assure la connectivité Internet nationale et internationale.

RSSI (Responsable de la Sécurité du Système d'Information) : nommé par le Président, il a pour mission l'élaboration et la mise en mise en œuvre de la politique de sécurité du système d'information de l'établissement.

SDSI (Schéma Directeur du Système d'Information) : plan stratégique du développement du système d'information.

SI (Système d'Information) : ensemble organisé de ressources (personnels, applications et équipements informatiques, données, procédures…) nécessaire au traitement de l'information, dans le cadre d'objectifs définis au niveau de la stratégie de l'établissement.

Spam (pollupostage ou pourriel en français) : courriel, généralement commercial, envoyé massivement à des listes d'adresses constituées frauduleusement.

Spyware (logiciel espion en français) : code malveillant généralement intégré à un programme légitime pour effectuer une action de collecte d'information ; par exemple ce qui est tapé au clavier pour récupérer des mots de passe (keylogger en anglais). Les informations ainsi récupérées sont ensuite automatiquement et discrètement envoyées au pirate ou celui-ci vient les chercher via une porte dérobée (backdoor en anglais).

SSI (Sécurité du Système d'Information) : ensemble des moyens techniques, organisationnels, juridiques et humains nécessaire et mis en place pour conserver, rétablir et garantir la sécurité du système d'information. La SSI a pour objet de contrer les menaces pesant sur le SI (environnement, pannes matérielles, erreurs humaines ou logicielles, attaques diverses...) par des mesures proportionnées aux risques.

USB (Universal Serial Bus) : norme de transmission de données (et d'énergie) entre un ordinateur et certains périphériques tels que les omniprésentes clés USB (mémoires amovibles).

Ver : logiciel malveillant se propageant à l'insu et sans intervention de l'utilisateur. Il tente d'infecter les ordinateurs de proche en proche via différents protocoles d'échanges entre ces machines. Par exemple par envoi automatique aux adresses contenues dans le carnet d'adresse pour un ver de type messagerie.

Virus : code malveillant intégré à des logiciels ou fichiers légitimes échangés par les utilisateurs (dans les pièces jointes aux messages électroniques par exemple). La nocivité d'un virus dépend du bon vouloir de son concepteur...