



**Université Pierre et Marie Curie
4 Place Jussieu
75252 PARIS Cedex 05**

**Charte de bon usage
du Système d'Information
de l'Université Pierre et Marie Curie**

Version 2.6.1 (Février 2011)

La présente « **charte de bon usage du système d'information de l'UPMC** » définit les conditions d'utilisation des ressources informatiques de l'établissement, et des ressources informatiques externes accessibles via le réseau informatique de l'établissement, dans le respect des lois et règlements en vigueur.

Elle précise les droits et devoirs de l'établissement et des personnels ayant accès au système d'information, quel que soit leur statut. Elle rappelle les responsabilités des utilisateurs et les règles qui doivent régir leur usage professionnel et privé : « nul ne doit abuser des ressources informatiques mises à sa disposition par l'Établissement pour l'accomplissement de ses missions ».

Elle précise dans une annexe les droits et devoirs spécifiques des administrateurs des systèmes, réseaux, applications et données qui bénéficient d'accès privilégiés au système d'information pour l'exercice de leur fonction.

Elle a pour vocation d'être diffusée à l'ensemble des personnels ainsi qu'aux utilisateurs occasionnels du système d'information de l'UPMC. Dans les lieux où ces ressources peuvent être utilisées par des personnes « de passage », les bibliothèques par exemple, elle devra être affichée ostensiblement.

C'est « **un code de bonne conduite** », élément de base de la politique de sécurité du système d'information, présentant une valeur juridique, puisqu'annexée au règlement intérieur de l'établissement.

Sommaire

Préambule	4
Article I. Champ d'application.....	5
Article II. Conditions d'utilisation du système d'information.....	5
Section II.1. Règles de base.....	5
Section II.2. Utilisation professionnelle / privée	5
Section II.3. Continuité de service : gestion des absences et des départs	6
Section II.4. Conformité aux règlements et lois en vigueur	6
Article III. Principes de sécurité	8
Section III.1. Règles de sécurité applicables.....	8
Section III.2. Devoirs de signalement et d'information	9
Section III.3. Mesures de contrôle de la sécurité	10
Article IV. Communication électronique.....	10
Section IV.1. Messagerie électronique.....	10
Section IV.2. Internet	12
Section IV.3. Spécificités : unité mixtes de recherche, unité classifiée.....	13
Article V. Journalisation des accès.....	13
Article VI. Limitation des usages et sanctions des abus	13
Article VII. Entrée en vigueur de la charte.....	13
Annexe I. Administrateurs de système d'information	14
Annexe I.1. Définition et mission d'un administrateur de système d'information.....	14
Annexe I.2. L'administrateur et la sécurité du système d'information.....	14
Annexe I.3. Droits et devoirs spécifiques.....	15
Annexe I.4. Alertes internes à l'entité.	16
Annexe I.5. Chaîne d'alerte de l'UPMC	16
Annexe I.6. Information des utilisateurs.....	17
Annexe I.7. Mesures conservatoires.....	17
Annexe II. Quelques références UPMC.....	18
Annexe III. Glossaire	19

Préambule

La présente charte définit les règles d'usages et de sécurité du système d'information que l'Université Pierre et Marie Curie et l'utilisateur s'engagent à respecter. Elle précise les droits et devoirs de chacun.

Par « *système d'information* » (SI) s'entend l'ensemble des moyens matériels, logiciels, applications, bases de données et réseaux de télécommunications, pouvant être mis à disposition par l'Université Pierre et Marie Curie. L'informatique nomade (clés USB, assistants personnels, ordinateurs portables, téléphones mobiles, etc.) est également un élément constitutif du système d'information.

Le terme « *utilisateur* » désigne toute personne ayant accès, dans le cadre de l'exercice de son activité professionnelle¹, aux ressources du système d'information quel que soit son statut. Il s'agit notamment de :

- tout agent titulaire ou non titulaire, vacataire, stagiaire, doctorants, hébergé, invité, personnel externe (incubateur, collaboration scientifiques, etc.) concourant à l'exécution des missions du service public de la recherche et de l'éducation ;
- tout prestataire² ayant un contrat avec l'Université Pierre et Marie Curie.

Le bon fonctionnement du système d'information suppose le respect des dispositions législatives et réglementaires concernant la sécurité, la performance des traitements et la conservation des données. La Politique de Sécurité du Système d'Information (PSSI)³ de l'UPMC s'applique à l'ensemble du système d'information de l'UPMC.

Engagements de l'Université Pierre et Marie Curie

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

L'Université Pierre et Marie Curie 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 Pierre et Marie Curie est tenue de respecter l'utilisation ponctuelle du système d'information à titre privé.

Engagements de l'utilisateur

L'utilisateur est responsable, en tout lieu, de l'usage qu'il fait du système d'information auquel il a accès. Il a une obligation de réserve et de confidentialité à l'égard des informations et documents auxquels il accède. Cette obligation implique le respect des règles d'éthique professionnelle et de déontologie⁴.

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

¹ Une charte spécifique encadre l'usage du SI par les étudiants de l'UPMC.

² Le contrat devra prévoir expressément l'obligation de respect de la charte.

³ La PSSI de l'UPMC est actuellement (septembre 2010) en cours d'élaboration.

⁴ Notamment le secret médical dans le domaine de la santé.

Article I. Champ d'application

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

L'annexe I encadre les missions d'administrateur de système d'information.

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

Section II.1. Règles de base

II.1.1. Conditions d'accès

Le droit d'accès d'un utilisateur aux ressources informatiques est soumis à autorisation. Ce droit est **personnel** et **incessible**. Il disparaît dès que son utilisateur ne remplit plus les conditions qui lui ont autorisé l'accès⁵.

II.1.2. Informations individuelles concernant l'utilisateur

Lors de sa demande d'accès au système d'information, chaque utilisateur est tenu de fournir des informations valides : adresses personnelle et/ou professionnelle, numéro de téléphone, entité⁶ de rattachement, etc. permettant de le contacter en cas d'incident informatique. Il s'engage à notifier toute modification de ces informations.

II.1.3. Respect du caractère a priori confidentiel des informations

En l'absence d'une autorisation explicite, toute tentative d'accès à des informations détenues par d'autres utilisateurs est considérée comme illicite⁷.

Section II.2. Utilisation professionnelle / privée

Le système d'information est destiné à des usages professionnels conformes aux missions de l'Université Pierre et Marie Curie (enseignement, recherche, valorisation, administration).

L'utilisation résiduelle du système d'information à titre privé est admise sous réserve qu'elle soit licite, non lucrative⁸ et raisonnable en termes de fréquence et de durée. Le surcoût qui en résulte doit demeurer négligeable au regard du coût global d'exploitation.

Il appartient à l'utilisateur de conserver ses données à caractère privé dans un espace prévu à cet effet en mentionnant le caractère privé sur la ressource⁹ de stockage. Toute autre information est réputée à usage professionnel. La sauvegarde des données à caractère privé est effectuée avec les données professionnelles lorsqu'elles figurent sur un espace inclus dans le plan de sauvegardes automatiques de

⁵ L'accès aux services de base (par exemple la messagerie) est généralement prolongé de 3 mois sauf demande contraire du responsable hiérarchique de l'utilisateur ou du responsable du service numérique.

⁶ On appelle « entité » toute composante administrative de l'université telle que : unité d'enseignement, unité de recherche, service administratif, bibliothèque, service commun, etc.

⁷ Sauf pour des raisons de continuité de service et pour accès à des données professionnelles. Cf. section II.3.

⁸ Cela exclut, entre autres, la pratique des « jeux d'argent et de hasard en ligne ».

⁹ Par exemple, "PRIVE-nom-de-la-ressource" : la « ressource » pouvant être un message, un fichier ou toute autre ressource numérique.

l'entité ; leur copie sur un support privé incombe à l'utilisateur. En l'absence de plan de sauvegardes automatiques, celles-ci doivent être effectuées par l'utilisateur. Il veillera alors à effectuer la copie régulière des données professionnelles sur un support fourni par l'entité et celle des données à caractère privé sur un support privé.

En cas de décès, les données à caractère privé figurant sur le poste de travail ou tout autre matériel informatique mis à disposition par l'UPMC, seront remises aux ayants droits, sur leur demande, au même titre que les affaires personnelles retrouvée sur le lieu de travail.

Section II.3. Continuité de service : gestion des absences et des départs

Aux seules fins d'assurer la continuité de service, l'utilisateur informe sa hiérarchie des modalités permettant l'accès aux ressources mises spécifiquement à sa disposition¹⁰.

L'utilisateur est responsable de son espace de données à caractère privé et il lui appartient de le détruire au moment de son départ. L'université s'engage à assurer la confidentialité des espaces privés (sauf cas prévus par la loi) pendant une durée de 3 mois, période pendant laquelle l'utilisateur pourra demander à y accéder et au delà de laquelle l'espace sera détruit par le Chargé de Sécurité du Système d'Information¹¹ (CSSI) de l'entité. Les données professionnelles restent à la disposition de l'employeur. L'utilisateur peut demander la redirection temporaire de ses courriels vers une adresse qu'il fournit¹².

Le droit d'accès aux données à caractère personnel figurant dans un fichier ou traitement mis en œuvre par l'UPMC, en son nom et pour son compte, s'éteint au décès de la personne concernée. Seule une demande de prise en considération du décès (avec les mises à jour qui en sont la conséquence) peut être effectuée par un ayant droit du défunt¹³.

Les mesures de conservation des données professionnelles sont définies avec le CSSI¹⁴ en conformité avec la PSSI de l'entité¹⁵.

Section II.4. Conformité aux règlements et lois en vigueur

II.4.1. Respect de la propriété intellectuelle

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

- utiliser les logiciels dans les conditions des licences souscrites (notamment effectuer les éventuelles copies de manière strictement conforme aux dispositions prévues) ;
- ne pas reproduire, copier, diffuser, modifier ou utiliser tout document numérique protégé 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.

¹⁰ Voir section III.1 les recommandations concernant les mots de passe.

¹¹ À défaut : par le directeur de l'entité ou une personne désignée par lui.

¹² L'adresse de redirection est entrée dans l'annuaire (modification de l' « Adresse électronique de délivrance du courrier ») par l'utilisateur lui-même ou par le « référent annuaire » de son entité ou sur demande à assistance-annuaire@upmc.fr. Intégrée à l'annuaire, cette redirection sera effective tant que l'utilisateur y figurera.

¹³ Cf. article 40 de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

¹⁴ À défaut : par le directeur de l'entité ou une personne désignée par lui.

¹⁵ À défaut : PSSI de l'établissement.

II.4.2. 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 dite « Informatique et Libertés ».

En conséquence, tout utilisateur souhaitant procéder à une telle création devra en accomplir les formalités préalables auprès du Correspondant Informatique et Libertés de l'Université Pierre et Marie Curie¹⁶ et informer les personnes concernées (type de données collectées, traitements, destinataires, etc.).

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 du traitement.

II.4.3. Respect de la législation concernant le droit à la vie privée

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

II.4.4. Respect des clauses contractuelles des ressources électroniques

L'accès aux ressources documentaires électroniques éditoriales doit s'effectuer dans les conditions contractuelles des licences souscrites par l'Université Pierre et Marie Curie.

II.4.5. Respect des lois concernant la diffusion de l'information

L'utilisation des moyens informatiques mis à disposition par l'Université Pierre et Marie Curie doit respecter la réglementation en vigueur. En particulier, la diffusion de messages diffamatoires ou injurieux, les provocations et apologies (crime, racisme, négationnisme, crimes de guerre, ...), l'accès, la détention, la diffusion d'images à caractère pédophile, la publication d'informations confidentielles sans autorisation préalable ou en violation du droit de la propriété intellectuelle sont strictement interdits.

II.4.6. Respect de la charte RENATER

Le Réseau National de télécommunications pour la Technologie, l'Enseignement et la Recherche (RENATER) fournit une connectivité nationale et internationale aux établissements de cette communauté à laquelle appartient l'UPMC. Les règles d'usage de RENATER (réseau réservé à une utilisation professionnelle) sont définies par une charte déontologique¹⁷ qui s'impose à tous les utilisateurs.

L'usage commercial à titre privé est proscrit.

¹⁶ Adresse : cil@upmc.fr.

¹⁷ Cf. http://www.renater.fr/IMG/pdf/charte_fr.pdf (version anglaise : http://www.renater.fr/IMG/pdf/charte_en.pdf).

Article III. Principes de sécurité

Section III.1. Règles de sécurité applicables

L'Université Pierre et Marie Curie met en œuvre les mécanismes de protection appropriés sur le système d'information mis à la disposition des utilisateurs.

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

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

- de respecter les consignes de sécurité¹⁸, notamment les règles relatives à la gestion des mots de passe¹⁹ ;
- de garder strictement confidentiels son (ou ses) mot(s) de passe et ne pas le(s) dévoiler à un tiers²⁰ ;
- de respecter la gestion des accès, en particulier ne pas utiliser les mots de passe d'un autre utilisateur, ni chercher à les connaître²¹ ;
- d'utiliser des mots de passe différents pour accéder à des environnements différents (sites universitaires, sites commerciaux, réseaux sociaux²²...) ou à des périmètres différents (utilisateur, administrateur, accès à une application spécifique...).

Le choix d'un mot de passe non trivial et son changement en cas de doute, notamment lorsqu'il a été utilisé à partir d'un poste connecté à un réseau extérieur non sécurisé, est une obligation pour l'utilisateur.

Si pour des raisons exceptionnelles et ponctuelles, un utilisateur se trouve dans l'obligation de communiquer son mot de passe personnel, il devra procéder, dès que possible, au changement de ce dernier ou en demander la modification à l'administrateur. Le bénéficiaire de la communication du mot de passe ne peut le communiquer à son tour à un tiers, ni l'utiliser en dehors de la circonstance exceptionnelle qui l'a conduit à en avoir connaissance.

¹⁸ Cf. PSSI, chartes de « bon usage », avis de sécurité, notes spécifiques, etc.

¹⁹ Il y a lieu de distinguer les mots de passe « personnels » donnant accès aux ressources informatiques en tant que « consommateur », des mots de passe « fonctionnels » protégeant l'accès aux ressources dont l'utilisateur est l'administrateur et ayant pour objectif d'offrir un service à une communauté. **L'utilisateur peut être amené exceptionnellement et ponctuellement à communiquer son mot de passe personnel lorsqu'aucun autre moyen d'accès aux données professionnelles qu'il protège n'est possible. Ce mot de passe ne doit pas être confié à quiconque (supérieur hiérarchique, collaborateur, intervenants divers...), hors d'une urgence critique et justifiée en termes de continuité de service, et sans l'accord du CSSI de l'entité ou, à défaut, du RSSI de l'établissement.** Le bénéficiaire n'est pas autorisé à accéder aux répertoires, données et messages dont le caractère privé est manifeste. Par ailleurs, on trouvera dans l'annexe I.3 de cette charte les bonnes pratiques en termes de politique de gestion des mots de passe « fonctionnels ».

²⁰ Sauf pour des raisons (cas de force majeure) de continuité de service et pour accès strictement limité aux données professionnelles. Voir note précédente.

²¹ À noter que l'hameçonnage (« phishing » en anglais) est une méthode courante pour obtenir frauduleusement un mot de passe. **Toute demande de mot de passe par courriel (avec réponse par le même canal ou en suivant un lien vers un formulaire web) est illégitime ; aucune suite ne doit y être donnée.**

²² À noter que les informations « confiées spontanément » à ces réseaux par leurs abonnés, peuvent être une précieuse source de renseignements pour les cyberdélinquants, facilitant usurpations d'identité et autres malversations d'ingénierie sociale (Cf. obligations de réserve et de confidentialité des agents de la fonction publique).

Par ailleurs et conformément à la PSSI, la protection des ressources mises à la disposition de l'utilisateur nécessite l'application d'un certain nombre de règles élémentaires :

de la part de l'Université Pierre et Marie Curie :

- 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 (Cf. Section II.3) ;
- limiter l'accès aux seules ressources pour lesquelles l'utilisateur est expressément habilité ;

de la part de l'utilisateur :

- ne pas abuser des ressources informatiques auxquelles il a accès²³ et être attentif à celles dont il a la responsabilité ;
- ne pas 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 rendre accessibles à des tiers les services qui lui sont offerts dans le cadre de son activité ;
- ne pas connecter aux réseaux locaux des équipements non autorisés par l'Université Pierre et Marie Curie ;
- ne pas installer, télécharger ou utiliser sur le matériel de l'Université Pierre et Marie Curie, des données, logiciels ou progiciels dont les droits de licence n'ont pas été acquittés, ou ne provenant pas de sites dignes de confiance ;
- ne pas déposer des données professionnelles (pour lesquelles a été identifié un besoin direct ou indirect de confidentialité) sur un serveur externe et/ou ouvert au grand public (Google, Free, Orange, ...) ou sur le poste de travail d'un autre utilisateur sans analyse de risques préalable réalisée en concertation avec le CSSI et validée par le directeur de l'entité ;
- se conformer aux dispositifs mis en place par l'Université Pierre et Marie Curie pour lutter contre les virus et les attaques par programmes informatiques ;
- ne pas nuire volontairement au bon fonctionnement des ressources informatiques et des réseaux par des manipulations anormales du matériel ou par l'introduction de logiciels malveillants ou intrusifs (virus, chevaux de Troie, bombes logiques, outils d'intrusion...). En cas d'usage contrevenant à cette interdiction pour des raisons justifiées, notamment dans le cadre d'un projet de recherche, une demande préalable devra être formulée auprès du Responsable de la Sécurité du Système d'Information (RSSI) de l'université ;
- assurer la protection des informations sensibles de l'unité et ne pas les transporter sans protection (telle qu'un chiffrement) sur des supports mobiles (ordinateurs portables, clés USB, disques externes, etc.) ;
- ne pas quitter son poste de travail, a fortiori un ordinateur en libre service, sans se déconnecter ou verrouiller sa session par un mot de passe.

Section III.2. Devoirs de signalement et d'information

L'Université Pierre et Marie Curie doit porter à la connaissance de l'utilisateur les éléments susceptibles de lui permettre d'apprécier le niveau de risque encouru dans l'utilisation du système d'information (PSSI, chartes, avis et alertes de sécurités, notes spécifiques, etc.).

L'utilisateur doit avertir le CSSI²⁴ de son entité dans les meilleurs délais en cas de découverte d'une anomalie affectant le système d'information, notamment une intrusion ou une tentative d'accès illicite à son propre compte.

²³ En particulier ne pas télécharger et stocker sur les équipements de l'établissement des fichiers privés volumineux tels que films, vidéos, musiques, etc. À noter que l'établissement dispose de serveurs spécialisés pour la diffusion des documents multimédia « enseignement et recherche ».

²⁴ À défaut : le RSSI de l'Université Pierre et Marie Curie (adresse : rsi@upmc.fr).

Section III.3. Mesures de contrôle de la sécurité

L'utilisateur est informé :

- que pour effectuer la maintenance corrective, curative ou évolutive, l'Université Pierre et Marie Curie se réserve la possibilité de réaliser des interventions (le cas échéant à distance) sur les ressources mises à sa disposition ;
- qu'une intervention à distance sur le poste de travail de l'utilisateur est précédée d'une information de ce dernier²⁵ ;
- que toute donnée bloquante pour le système ou générant une difficulté technique d'acheminement à son destinataire, sera isolée ; le cas échéant supprimée.

L'Université Pierre et Marie Curie informe l'utilisateur que le système d'information peut donner lieu à une surveillance et un contrôle à des fins statistiques, de traçabilité²⁶, d'optimisation, de sécurité ou de détection des abus, dans le respect de la législation applicable.

Les personnels chargés des opérations de contrôle du système d'information sont soumis à l'obligation de discrétion. Ils ne peuvent divulguer les informations qu'ils sont amenés à connaître dans le cadre de leurs fonctions dès lors que ces informations sont couvertes par le secret des correspondances ou qu'identifiées comme telles, elles relèvent de la vie privée de l'utilisateur. En revanche, ils doivent communiquer ces informations au CSSI²⁷ de leur entité si elles mettent en cause le bon fonctionnement technique des applications ou leur sécurité, ou aux autorités compétentes si elles tombent dans le champ de l'article 40 alinéa 2 du code de procédure pénale²⁸.

Article IV. Communication électronique

Section IV.1. Messagerie électronique

La messagerie est un moyen de communication ouvert à des usages professionnels contribuant aux missions de l'université (enseignement, recherche, valorisation, administration) ; elle peut constituer le support d'une communication privée telle que définie à la section II.2. Cependant, à cette fin, l'université recommande l'utilisation d'adresses de messagerie privées.

IV.1.1. Adresses électroniques

L'Université Pierre et Marie Curie 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.

Une adresse électronique, fonctionnelle ou organisationnelle, peut être mise en place pour un utilisateur ou un groupe d'utilisateurs pour les besoins de l'Université Pierre et Marie Curie²⁹.

²⁵ Par exemple par l'ouverture d'une fenêtre sur l'écran demandant l'acquiescement de l'utilisateur.

²⁶ Cf. Politique de Gestion des Journaux Informatiques de l'Université Pierre et Marie Curie.

²⁷ À défaut : au RSSI de l'Université Pierre et Marie Curie.

²⁸ 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.

²⁹ Cette option est recommandée puisqu'elle facilite grandement la continuité du service assuré par un personnel absent ou ayant quitté l'établissement par redirection instantanée de sa messagerie « fonctionnelle » vers le(la) remplaçant(e).

La gestion d'adresses électroniques correspondant à des listes de diffusion institutionnelles, désignant une catégorie d'utilisateurs, relève de la responsabilité exclusive de l'Université Pierre et Marie Curie : ces listes ne peuvent être utilisées sans autorisation explicite.

IV.1.2. Contenu des messages électroniques

Tout message est réputé professionnel sauf s'il comporte une mention particulière et explicite indiquant son caractère privé³⁰ ou s'il est stocké dans un espace privé de données.

Pour préserver le bon fonctionnement des services, des limitations³¹ peuvent être mises en place : dans ce cas, les termes en sont précisés et portés à la connaissance de l'utilisateur de la messagerie.

Les messages comportant des contenus à caractère illicite quelle qu'en soit la nature (Cf. Section II.4) sont interdits.

L'utilisateur doit veiller à ce que la taille des messages reste raisonnable³² et à ce que leur diffusion soit limitée aux seuls destinataires concernés afin d'éviter les envois de messages en masse³³, l'encombrement inutile de la messagerie ainsi qu'une dégradation (saturation) du service.

IV.1.3. 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 articles³⁴ 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.

IV.1.4. Stockage et archivage des messages

Les serveurs de messagerie effectuent la sauvegarde temporaire³⁵ des boîtes à lettres en prévention des erreurs de manipulation des utilisateurs et des pannes des équipements. Cette sauvegarde ne garantit pas le recouvrement de l'ensemble des messages reçus (exemple : message détruit entre le moment de son arrivée et celui de sa sauvegarde). Les utilisateurs devront pouvoir effectuer la restauration ou la destruction des messages sauvegardés³⁶.

Chaque utilisateur doit organiser et mettre en œuvre les moyens nécessaires à l'archivage des messages pouvant être indispensables ou simplement utiles en tant qu'éléments de preuve.

³⁰ Par exemple, les messages comportant les termes « privé » ou « personnel » dans l'objet ou sujet du message.

³¹ Exemple : mécanisme de filtrage des courriels indésirables (« antispam »).

³² La messagerie n'est pas la seule possibilité d'échange de fichiers. Les espaces partagés sont, par exemple, une alternative préférable pour l'échange des gros fichiers avec un groupe d'utilisateurs.

³³ Notamment l'envoi de courriels indésirables (« spam »), la participation à des chaînes de lettres, le relais de canulars (« Hoax »), etc.

³⁴ Issus de la loi n° 2004-575 du 21 juin 2004, ces articles fixent certaines obligations pour la conclusion des contrats en ligne.

³⁵ Les utilisateurs doivent être informés de la politique de messagerie (filtrages ; procédures de sauvegarde et de restauration ; procédure de destruction de la copie/sauvegarde d'un message si l'opération est possible, durée de conservation ; etc.), dépendante de l'administration du serveur/service hébergeant leur boîte à lettres.

³⁶ La restauration suppose qu'il y ait eu sauvegarde (ce qui n'est pas le cas entre l'arrivée du message et l'exécution du processus périodique de sauvegarde) et la destruction du message sauvegardé suppose que la technologie le permette aisément (ce qui n'est par exemple pas le cas pour des sauvegardes sur bandes magnétiques).

Section IV.2. Internet

L'université Pierre et Marie Curie offre un accès à l'intranet de l'établissement ainsi qu'à l'ensemble du réseau Internet pour un usage dédié à la réalisation de ses missions (enseignement, recherche, valorisation et administration). Une utilisation résiduelle privée, telle que définie en section II.2, est admise. Il est rappelé qu'Internet est soumis à l'ensemble des règles de droit en vigueur.

IV.2.1. Publication sur les sites internet et intranet de l'Université Pierre et Marie Curie

Toute publication de pages d'information sur les sites internet ou intranet de l'Université Pierre et Marie Curie doit être validée par un responsable de site ou responsable de publication³⁷.

Sauf autorisation explicite de l'établissement, il est interdit d'employer la charte graphique et le logo de l'UPMC (ou tout autre apparence approchante) hors des serveurs du domaine « upmc.fr ».

La mise en ligne de cours UPMC devra de préférence s'effectuer à partir des serveurs prévus à cet effet.

Aucune information relative aux spécificités du système d'information de l'Université Pierre et Marie Curie ne doit être publiée sans autorisation préalable.

Les pages dites « personnelles-professionnelles », dont la publication est autorisée,

- sont des pages Web du domaine « upmc.fr » (ou d'un de ses sous-domaines) placées sous la responsabilité d'une entité de l'université ou d'une association autorisée. Elles doivent être fiables et l'on doit pouvoir facilement les dater et identifier leur auteur ;
- contiennent exclusivement des informations de nature professionnelle, en rapport avec le métier du personnel ou avec les missions de l'université Pierre et Marie Curie ;
- concourent à l'image de l'université et des autres tutelles dans le cas des unités mixtes de recherche.

IV.2.2. Sécurité

L'accès Internet n'est autorisé qu'au travers des dispositifs de sécurité mis en place par l'Université Pierre et Marie Curie.

En cas d'incident, l'Université Pierre et Marie Curie se réserve le droit, avec information au plus tôt des utilisateurs³⁸, 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.

L'utilisateur est informé des risques et limites inhérents à l'utilisation d'Internet par le biais de la présente charte, de la PSSI, de notes spécifiques et d'actions de formations ou de campagnes de sensibilisation.

IV.2.3. Téléchargements et « mises en ligne »

Tout téléchargement de fichiers, notamment de sons ou d'images, sur Internet doit s'effectuer dans le respect des règlements et lois en vigueur (Cf. sous-section II.4).

L'Université Pierre et Marie Curie 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 (virus

³⁷ Cf. mentions légales du site web.

³⁸ Directement auprès du(des) utilisateur(s) concerné(s) pour les incidents spécifiques ; via les administrateurs système et réseaux des entités et/ou les listes de distributions spécialisées (ex : « securite@listes.upmc.fr », liste des correspondants sécurité des entités).

susceptibles d'altérer le bon fonctionnement du système d'information de l'Université Pierre et Marie Curie, codes malveillants, programmes espions, etc.).

La mise en œuvre d'un serveur accessible de l'extérieur doit être déclarée à la Direction du Système d'Information, administratrice du réseau, pour en autoriser l'accès. La « mise en ligne » de textes, de sons, d'images, de vidéos, de logiciels et tous autres documents doit s'effectuer dans le respect des règlements et lois en vigueur (Cf. sous-section II.4) et être en rapport avec les missions de l'Université Pierre et Marie Curie. Le nommage et la charte graphique du site devront suivre les règles définies par l'établissement.

Section IV.3. Spécificités : unité mixtes de recherche, unité classifiée...

Certaines entités, notamment les unités mixtes de recherche, peuvent imposer des restrictions d'accès en raison d'un niveau de sécurité plus élevé ou classifié défense. Des règles spécifiques figurent alors dans la PSSI de ces unités.

Article V. Journalisation des accès

L'Université Pierre et Marie Curie est dans l'obligation légale de mettre en place un système de journalisation³⁹ des accès Internet, de la messagerie et des caractéristiques des données échangées. La gestion des journaux informatiques (finalités, contenus, traitements, droits d'accès, destinataires, délais de conservation...) est conforme aux règles énoncées dans un document spécifiques⁴⁰ et à leur déclaration auprès de la Commission Nationale de l'Informatique et des Libertés⁴¹ en application de la loi n° 78-17 du 6 janvier 1978 modifiée.

Article VI. Limitation des usages et sanctions des abus

En cas de non-respect des règles définies dans la présente charte, 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 extra-professionnelles est passible de sanctions. Outre les sanctions pénales prévues par le code pénal (amendes et/ou emprisonnement), les personnels encourent des sanctions disciplinaires conformément aux dispositions législatives, réglementaires et statutaires en vigueur.

Article VII. Entrée en vigueur de la charte

La présente charte a été approuvée par le Conseil d'Administration de l'Université Pierre et Marie Curie le 29 novembre 2010. Elle est intégrée au règlement intérieur.

Mises à jour :

- février 2011 : clarification de procédure en cas de décès d'un utilisateur (Section II.2 et II.3).

³⁹ Conservation des informations techniques de connexion telles que l'heure d'accès, l'adresse IP de l'utilisateur, etc.

⁴⁰ « Politique de gestion des journaux informatiques à l'Université Pierre et Marie Curie », novembre 2009.

⁴¹ Déclaration effectuée auprès du Correspondant Informatique et Libertés de l'Université Pierre et Marie Curie.

Annexe I. Administrateurs de système d'information⁴²

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 Pierre et Marie Curie.

Cette annexe est indissociable de la « **Charte de bon usage du système d'information de l'Université Pierre et Marie Curie** » qu'elle complète en précisant les droits et devoirs des administrateurs de système d'information.

Annexe I.1. Définition et mission d'un administrateur de système d'information

Le terme « *administrateur* » désigne toute personne, employée ou non par l'UPMC, chargée explicitement⁴³ du bon fonctionnement et de la sécurité de ressources informatiques⁴⁴ 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 RSSI⁴⁵ 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.

Annexe I.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 service⁴⁶. 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 confidentielle⁴⁷, si ces données ne sont pas protégées par un mécanisme de chiffrement ; il est alors soumis au devoir de confidentialité (voir Annexe I.3)

Les équipements, systèmes, applications, ainsi que les outils dont l'administrateur fait usage dans l'exercice de sa fonction, sont exclusivement professionnels et autorisés⁴⁸ par l'UPMC. 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.

⁴² Dans la suite du document la locution « administrateur de système d'information » désigne les administrateurs des systèmes, réseaux, données et applications.

⁴³ Lettre de mission, profil de poste, contrat de travail, contrat de prestation de service, etc.

⁴⁴ Équipements réseau, serveurs, systèmes d'exploitation, applications, etc.

⁴⁵ Validée par l'Autorité Qualifiée pour la Sécurité du Système d'Information (AQSSI) de l'Université Pierre et Marie Curie c'est-à-dire son Président.

⁴⁶ Conformément au Plan de Continuité d'Activité (PCA) ou Plan de Reprise d'Activité (PRA).

⁴⁷ Informations à caractère personnel, espaces de données privées, données sensibles telles que résultats de recherche, contrats, brevets, notes d'examens, etc.

⁴⁸ Ou nécessitant une autorisation préalable comme, par exemple, l'installation de points d'accès sans fil.

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

Enfin, l'administrateur est responsable de la mise à jour⁴⁹ des systèmes, applications et dispositifs de sécurité⁵⁰, (nouvelles versions, correctifs de sécurité,...) 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 procédures⁵¹ qu'il met en place pour l'administration des services vitaux.

Annexe I.3. Droits et devoirs spécifiques

L'administrateur est soumis à la présente « Charte de bon usage ». Il doit, d'une manière générale, respecter les règles d'éthique professionnelle, 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 détecter 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 »⁵² sous réserve des dispositions prévues à la Section II.3 (continuité de service)⁵³ ;

⁴⁹ 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-cn/il/actu-cn/il/article/article//10-conseils-pour-securiser-votre-systeme-dinformation-1>), etc.

⁵⁰ Équipements et logiciels assurant la sécurité du système d'information dont, le cas échéant, les anti-virus.

⁵¹ Exemples : livre de bord à jour, scénario de redémarrage d'un système, etc.

⁵² Les droits d'accès « étendus » au système d'information renforcent le besoin de confidentialité de ce mot de passe.

⁵³ 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, CSSI, 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.

- 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'UPMC⁵⁴ 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'UPMC⁵⁵ ;
- 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 vigueur⁵⁶ ;
- 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 (Cf. Section II.4) sur les équipements, systèmes ou applications dont il a la responsabilité en isolant le composant en cause (fichier, serveur...), et en informant le CSSI⁵⁷ ;
- de veiller au respect, par les utilisateurs, de la présente « Charte de bon usage » et des consignes de sécurité figurant dans la PSSI.

Annexe I.4. Alertes internes à l'entité.

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 CSSI⁵⁸ 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 de bon usage 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.

Annexe I.5. Chaîne d'alerte de l'UPMC

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'UPMC lorsque les ressources informatiques dont il a la responsabilité sont concernées ;

⁵⁴ Elle est constituée de la Personne Juridiquement Responsable (le Président), du RSSI de l'établissement et du CSSI de l'entité.

⁵⁵ En conformité avec la loi dite « Informatique et Libertés ».

⁵⁶ La liste des traitements de données à caractère personnel de l'UPMC est tenue à jour par le Correspondant Informatique et Libertés (CIL).

⁵⁷ À défaut le RSSI.

⁵⁸ Le CSSI ou, à défaut, le RSSI avise en fonction de la nature et de la gravité de l'incident (sans suite / information de la direction de l'entité / remontée confidentielle de la chaîne fonctionnelle de sécurité / ...)

- fournir au CSSI 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 CERT⁵⁹ et aux consignes du CSSI⁶⁰, 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.

Annexe I.6. 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'UPMC et du réseau RENATER, les sensibiliser aux problèmes de sécurité informatique, leur faire connaître les consignes techniques de sécurité, en appui des actions du CSSI.

Annexe I.7. 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.

⁵⁹ Cf. « Que faire en cas d'incident ».

⁶⁰ Exemple : mode de conservation des traces d'un incident.

Annexe II. Quelques références UPMC⁶¹

Serveur institutionnel de l'établissement :

<http://www.upmc.fr>

Serveur intranet de l'établissement :

<http://www.upmc.fr/fr/intranet.html>

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

rssi@upmc.fr

Adresse du pôle SSI de la DSI

pole-ssi@listes.upmc.fr

Pages intranet « Sécurité du système d'information » :

http://www.upmc.fr/fr/intranet/e_administration/securite_systemes_d_information.html

Adresse du correspondant informatiques et libertés (CIL) :

cil@upmc.fr

Pages intranet « Informatique et libertés » :

http://www.upmc.fr/fr/intranet/e_administration/informatique_et_libertes.html

Direction du système d'information :

<http://www.dsi.upmc.fr>

TICE / Centre de production multimédia :

http://www.upmc.fr/fr/formations/tice/centre_de_production_multimedia.html

⁶¹ Ces références peuvent être modifiées ; la version en ligne de ce document sera maintenue à jour.

Annexe III. 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.

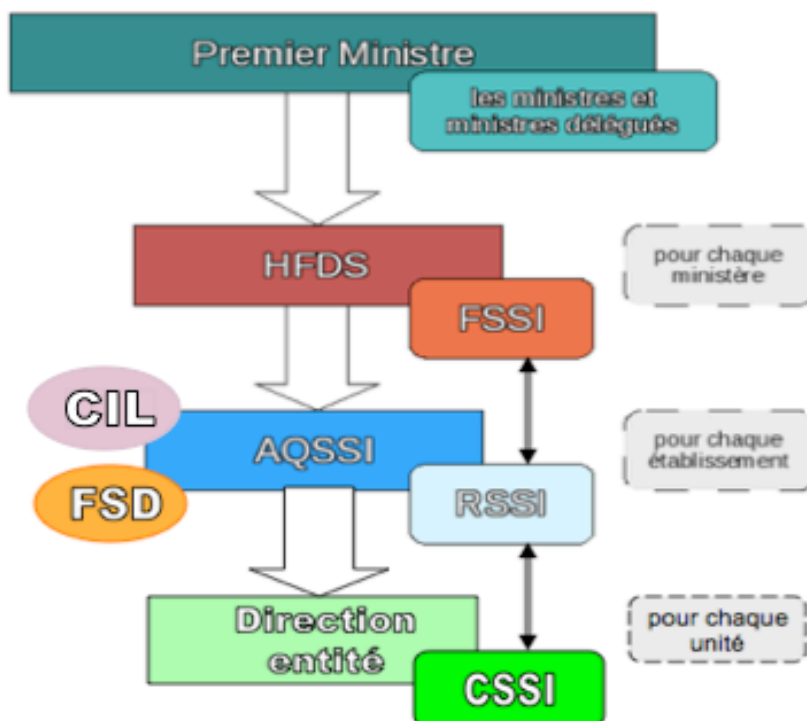
Antivirus : logiciels conçus pour détecter et éliminer des codes malveillants tels que virus, vers, chevaux de Troie. Basés sur une recherche de « signatures » (partie de code spécifique), ils sont mis en œuvre sur les passerelles de messagerie et/ou les postes de travail.

AQSSI (Autorité Qualifiée pour la Sécurité du Système d'Information) : elle définit la politique de sécurité du système d'information adaptée à son organisme, en fixe les objectifs et les moyens. Ce rôle est tenu par le chef d'établissement.

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.

Chaîne fonctionnelle de la sécurité du système d'information : créée par la directive interministérielle 901 :



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.

CoStraSI : Le Comité Stratégique du Système d'Information de l'UPMC coordonne et pilote le développement du SI de l'UPMC.

CSSI (Chargé de la Sécurité du Système d'Information) : nommé par le responsable de l'entité, il est chargé de la mise œuvre de la sécurité du système d'information de l'unité d'enseignement, de recherche ou administrative auquel il appartient.

DSI (Direction du Système d'Information) : service en charge du système d'information de l'UPMC (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.

FSD (Fonctionnaire de Sécurité et de Défense) : correspondant local du HFDS, il chargé par le Président de la protection du patrimoine scientifique et technique de l'établissement (mesures de défense, de vigilance, de prévention de crise et de situation d'urgence (plans Vigipirate, pandémies grippales...)).

FSSI (Fonctionnaire de la Sécurité des Systèmes d'Information) : il est chargé par le HFDS

- de porter la réglementation interministérielle relative à la sécurité des systèmes d'information à la connaissance des organismes concernés et d'en préciser les modalités d'application ;
- d'élaborer la réglementation propre à son ministère en définissant, pour chaque type de système d'information, les mesures de protection nécessaires ;
- de contrôler au sein du ministère l'application de cette réglementation et l'efficacité des mesures prescrites.

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.

HFDS (Haut Fonctionnaire de Défense et de Sécurité) : nommé par le Ministre, le HFDS anime et coordonne la politique du ministère et des établissements sous tutelle en matière de défense, de vigilance, de prévention de crise et de situation d'urgence (terrorisme, pandémie, catastrophe naturelle...).

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 œuvre –après validation par le CoStraSI et sur décision de l'AQSSI- 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* » [wikipedia]. 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...