Charte de bon usage du Système d'Information à l'attention des étudiants de l'Université Pierre et Marie Curie

La présente charte définit les règles d'usage et de sécurité du Système d'Information (SI) que l'Université Pierre et Marie Curie (UPMC) met à la disposition de ses étudiants.

Les droits d'accès aux ressources informatiques de l'Université ne sont octroyés qu'après l'engagement de respecter la présente charte et pourront être suspendus ou retirés dès lors que l'utilisateur dérogera à ces obligations ou enfreindra la loi.

Le « *système d'information* » est composé de l'ensemble des moyens matériels, logiciels, applications, bases de données et réseaux de télécommunications, pouvant être mis à disposition par l'UPMC. Le terme « *utilisateur* » désigne tout étudiant, apprenti ou stagiaire, régulièrement inscrit à l'UPMC, ayant accès aux ressources du SI dans le cadre d'une formation dispensée par l'établissement[1] : formation initiale ou formation tout au long de la vie, scientifique ou médicale, formation doctorale, CFA, école d'ingénieur, etc. Les étudiants « préinscrits » sont *utilisateurs* de certains services du SI de l'UPMC.

Conditions d'utilisation

Tout utilisateur est responsable de l'utilisation qu'il fait des ressources informatiques et s'engage à n'effectuer aucune opération susceptible de porter atteinte de quelque façon que ce soit :

- à l'intégrité, la sécurité, la disponibilité du SI de l'UPMC ;
- à l'image de l'UPMC ;
- au respect de la vie privée, au droit à l'image, au droit d'auteurs et droits voisins de toute personne physique ou morale, privée ou publique ;
- à l'ordre et à la sécurité publique ;
- aux biens et personnes par des faits constitutifs d'infractions pénales.

Accès au SI : L'utilisation des ressources informatiques de l'UPMC, qui suppose l'approbation de la présente charte, est soumise à autorisation préalable. Elle peut être retirée, partiellement ou totalement, temporairement ou définitivement, en cas de non respect de la charte.

Le droit d'accès aux ressources informatiques est **personnel** et **incessible**. Il disparaît dès que son utilisateur ne remplit plus les conditions qui lui ont autorisé l'accès[2].

Usage « étudiant » : Les moyens informatiques de l'UPMC mis à la disposition des utilisateurs sont destinés à une utilisation dans le cadre de leur formation. Il doit être fait un usage raisonnable de toutes les ressources informatiques partagées : puissance de calcul, espace disque, logiciels à jetons, bande passante sur le réseau, occupation des postes de travail...

L'utilisation d'équipements ou de logiciels non fournis par l'établissement engage la responsabilité de l'utilisateur et ne peut être tolérée que si :

- le rapport avec les études suivies est effectif ;
- la légalité de l'utilisation est incontestable ;
- la disponibilité, l'intégrité et la confidentialité du SI sont préservées.

[1] Une charte spécifique encadre l'usage du SI par les diplômés de l'UPMC qui souhaitent bénéficier des services numériques ouverts à leur intention par l'établissement.

[2] À défaut de réinscription à l'UPMC, l'accès aux services de base (par exemple la messagerie) est généralement prolongé jusqu'à la fin de l'année civile de la dernière inscription administrative, sauf demande contraire de la direction des études ou des responsables des services numériques concernés.

Une adresse électronique « @etu.upmc.fr » est attribuée à tout utilisateur[3]. La plus grande correction doit être respectée dans les échanges électroniques. Les contenus doivent être conformes aux lois et règlements en vigueur (voir plus loin). L'UPMC utilisera exclusivement cette adresse pour tous les échanges officiels. L'UPMC établira, lors de la création de la boîte à lettres « @etu.upmc.fr », une redirection automatique depuis cette boîte à lettres institutionnelle vers la boîte à lettres privée de l'utilisateur. Les utilisateurs ne souhaitant pas bénéficier de cette redirection automatique peuvent la supprimer à tout moment et sont alors invités à consulter régulièrement leur boîte à lettres « @etu.upmc.fr ». L'adresse privée de l'utilisateur sera utilisée par l'établissement lors de la phase « préinscription » (adresse institutionnelle non encore disponible) ou en cas de circonstances exceptionnelles[4].

Usage privé : L'utilisation résiduelle du SI à titre privé est tolérée sous réserve qu'elle soit éthique, licite, non lucrative, conforme à la charte déontologique RENATER[5] et raisonnable en termes de fréquence et de durée.

Conformité aux lois et règlements : l'utilisateur s'engage à un usage du SI de l'UPMC conforme aux lois et règlements en vigueur :

- propriété intellectuelle : utilisation des logiciels et des données dans les conditions des licences souscrites. Ne pas télécharger, reproduire, copier, diffuser, modifier ou utiliser tout document numérique (texte, image, son, vidéo, etc.) protégé par le droit d'auteur ou un droit voisin, sans avoir obtenu préalablement l'autorisation des titulaires de ces droits. Respect du droit des marques ;
- diffusion de l'information : sont interdits les messages diffamatoires, discriminatoires 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 ;
- 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 ;
- informatique et libertés : tout traitement de données nominatives est soumis à déclaration préalable auprès du Correspondant Informatique et Libertés de l'UPMC (cil@upmc.fr) ;
- l'utilisation des moyens informatiques mis à disposition par l'UPMC doit être conforme à la charte déontologique RENATER. Toute utilisation commerciale à titre privé est interdit ;
- respect des clauses contractuelles des ressources électroniques éditoriales, et des licences d'usage des logiciels, souscrites par l'UPMC.

Rappel des principales dispositions légales eu égard à l'objet de la présente charte

L'utilisateur s'engage à ne commettre aucune infraction aux dispositions légales et réglementaires en vigueur, notamment :

La législation relative à la protection des systèmes informatiques notamment les articles 323-1 à 323-7 du Code Pénal :

- le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 30000 euros d'amende. Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de 45000 euros d'amende ;
- le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de cinq ans d'emprisonnement et de 75000 euros d'amende ;

[3] Administrativement inscrit à une formation diplômante (diplôme d'état ou d'université).
[4] Par exemple en cas de problème avec l'adresse institutionnelle ou (ré)envoi du mot de passe associé.
[5] RENATER, le Réseau National de télécommunications pour la Technologie, l'Enseignement et la Recherche, fournit la connectivité Internet nationale et internationale de l'UPMC. Voir sa charte http://www.renater.fr/IMG/pdf/charte_fr.pdf (version anglaise : http://www.renater.fr/IMG/pdf/charte_en.pdf).

- le fait d'introduire frauduleusement des données dans un système de traitement automatisé ou de supprimer ou de modifier frauduleusement les données qu'il contient est puni de cinq ans d'emprisonnement et de 75000 euros d'amende ;
- la tentative des délits prévus par les articles 323-1 à 323-3-1 est punie des mêmes peines.

Les personnes physiques coupables des délits prévus au présent chapitre encourent également des peines complémentaires, notamment l'interdiction, pour une durée de cinq ans au plus, des droits civiques, civils et de famille, et l'interdiction, pour une durée de cinq ans au plus, d'exercer une fonction publique ou d'exercer l'activité professionnelle ou sociale dans l'exercice de laquelle ou à l'occasion de laquelle l'infraction a été commise.

La législation relative à la protection des droits de propriété intellectuelle notamment les articles L335-1 à 335-10 du Code de la propriété intellectuelle : les dispositions interdisent notamment à tout utilisateur de réaliser des copies de logiciels commercialisés, pour quelque usage que ce soit, ainsi que de dupliquer, distribuer ou diffuser des documents (images, sons, vidéos,...) protégés, ou d'altérer la protection d'une œuvre, d'un phonogramme, d'un vidéogramme ou d'un programme par un décodage, un décryptage ou toute autre intervention personnelle destinée à contourner, neutraliser ou supprimer un mécanisme de protection ou de contrôle.

La législation relative à la protection des données à caractère personnel, notamment les articles 50 à 52 de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés : les infractions aux dispositions de la loi de 1978 sont prévues et réprimées par les articles 226-16 à 226-24 du code pénal.

Voir quelques autres références législatives et réglementaires en annexe.

Règles de sécurité applicables

Conformément à la Politique de Sécurité du SI[6] de l'UPMC, la protection des ressources mises à la disposition de l'utilisateur nécessite l'application d'un certain nombre de règles élémentaires :

- choisir un mot de passe complexe[7], le garder strictement confidentiel et le changer en cas de doute sur sa confidentialité ; utiliser des mots de passe différents pour accéder à des environnements différents (sites universitaires, sites commerciaux, réseaux sociaux…) ;
- respecter la gestion des accès, en particulier ne pas utiliser les mots de passe d'un autre utilisateur, ni chercher à les connaître[8] ;
- ne pas tenter d'accéder à des ressources du SI, à des informations détenues par d'autres utilisateurs et aux communications entre tiers pour lesquelles il n'a pas d'autorisation explicite. Il faut noter que la capacité d'accéder à une information n'implique pas que l'accès soit effectivement autorisé ;
- ne pas rendre accessibles à des tiers les services qui lui sont offerts dans le cadre de sa formation ;
- ne pas publier les documents de l'UPMC auxquels il a accès dans le cadre de sa formation (sujets ou corrigés d'examen, supports de cours, etc.) sous quelque forme que ce soit. En ce qui concerne une éventuelle publication de notes de cours[9], aucune confusion ne doit être possible quant à leur origine et à l'absence d'assentiment de l'enseignant ;
- se conformer aux dispositifs mis en place par l'UPMC pour lutter contre les virus et les attaques par programmes informatiques et se conformer aux recommandations des administrateurs des systèmes informatiques ;

[6] La PSSI de l'UPMC est actuellement en cours d'élaboration.

[7] Minimum 10 caractères, mélange de lettres majuscules et minuscules, de chiffres et, si possible, de caractères spéciaux, paraissant aléatoire ou dénué de sens pour tout autre personne que son propriétaire (voir par exemple http://www.securite-informatique.gouv.fr/autoformations/motdepasse/co/Mots_de_Passe_CH01_SCH02.html).

[8] 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.**

[9] L'UPMC peut mettre à disposition de groupes d'étudiants des espaces de publication à accès réservé aux seuls étudiants de l'université.

- signaler aux administrateurs toute anomalie ou dysfonctionnement des systèmes informatiques, notamment tout ce qui concerne la sécurité du SI ;
- 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...) ;
- **ne pas quitter son poste de travail sans se déconnecter**.

Mesures de contrôle de la sécurité

L'utilisateur est informé que :

- l'UPMC met en œuvre les mécanismes de protection appropriés sur le SI mis à la disposition des utilisateurs ;
- l'UPMC exerce une surveillance et un contrôle de son SI à des fins de sécurité et de détection des abus, de statistiques d'usage et d'optimisation des ressources, dans le respect de la législation applicable ;
- conformément à la législation en vigueur[10] en termes de traçabilité, l'UPMC a mis en œuvre un système de journalisation[11] des sessions des utilisateurs de son SI. La gestion des journaux informatiques est conforme aux règles énoncées dans un document spécifiques[12] et à leur déclaration auprès du CIL de l'UPMC. Un extrait de ces journaux, en rapport avec l'objet d'une enquête en cours, peut être remis à l'autorité judiciaire à sa demande ;
- l'UPMC se réserve le droit de limiter la diffusion et le téléchargement massifs de fichiers et courriers électroniques dès lors que cela peut être attentatoire à la sécurité du SI, à la responsabilité juridique de l'établissement et à son image ;
- toute donnée bloquante pour le système ou générant une difficulté technique sera isolée ; le cas échéant supprimée ;
- en cas d'incident, l'UPMC se réserve le droit, avec information au plus tôt des utilisateurs, de filtrer ou d'interdire l'accès à certains sites ou l'usage de certains protocoles de communication.

Les personnels de l'UPMC chargés des opérations de contrôle du SI sont soumis à l'obligation de discrétion. Cependant ils doivent communiquer les informations aux autorités compétentes si elles tombent dans le champ de l'article 40 alinéa 2 du code de procédure pénale[13].

Sanctions des abus

En cas de non-respect des règles définies dans la présente charte, le Président de l'UPMC pourra par mesure conservatoire et sans préjudice des poursuites civiles ou pénales, et des procédures disciplinaires pouvant être engagées à l'encontre de l'utilisateur, prendre toute mesure utile à la préservation de ses intérêts et des intérêts des personnels, usagers, partenaires publics et privés, ou tiers, notamment :

- limiter les usages du SI ;
- interdire tout accès au SI de l'UPMC ;
- procéder à toute mesure d'investigation sur les ressources informatiques matérielles et immatérielles mises à disposition par l'UPMC ainsi que dans leurs échanges avec l'extérieur.

L'Université est également tenue par la loi de signaler aux services répressifs compétents toute violation des lois constatée.

La présente charte a été votée par le Conseil d'Administration de l'UPMC le 10 avril 2012. Elle est annexée au règlement intérieur.

[10] Loi n° 2004-575 du 21 juin 2004 dite « pour la confiance dans l'économie numérique » (LCEN).
[11] « log » en anglais.
[12] « Politique de gestion des journaux informatiques à l'Université Pierre et Marie Curie », novembre 2009.
[13] 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.

Annexe : Principales références législatives et réglementaires

Loi du 29 juillet 1881 modifiée relative à la liberté de la presse (notamment chapitre IV : Des crimes et délits commis par la voie de la presse ou par tout autre moyen de publication).

Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi 2004-801 du 6 août 2004 (cf. articles 226-16 à 226-24 et R625-10 du code pénal).

Loi n° 88-19 du 5 janvier 1988 relative à la fraude informatique dite "loi Godfrain" (cf. articles 323-1 à 323-7 du code pénal).

Code pénal, notamment les articles 226-1 et suivants relatifs à l'atteinte à l'intimité de la vie privée, **les articles 226-15 et suivants** relatifs au secret des correspondances, **l'article 227-23** relatif à la détention et/ou la diffusion de documents à caractère pédophiles et l'**article 227-24** relatif à la diffusion et/ou au commerce de messages à caractère violent ou pornographique ou de nature à porter gravement atteinte à la dignité humaine.

Code Civil, notamment les articles relatifs au droit à l'image et à la protection de la vie privée.

Loi n° 85-660 du 3 juillet 1985 relative aux droits d'auteur, a étendu aux logiciels en tant qu'œuvres de l'esprit, la protection prévue par la loi n° 57-298 du 11 mars 1957 sur la propriété littéraire et artistique. (cf. **Code de la Propriété Intellectuelle**, œuvres définies par l'article L112-2, articles L335-2 et suivants sur la contrefaçon des œuvres de l'esprit, article L521-1 et suivants sur la contrefaçon des dessins ou modèles nationaux, article L713-1 et suivants sur la protection des marques).

Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (LCEN) et le **décret n° 2011-219** relatif à la conservation et à la communication des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne.

Loi n° 2009-669 du 12 juin 2009 a créé l'HADOPI chargée 1) de protéger les œuvres à l'égard des actes de contrefaçon numérique 2) encourager le développement de l'offre légale et observer l'utilisation licite et illicite des œuvres 3) assurer une régulation et une veille dans le domaine des mesures techniques ; complétée par la loi n° 2009-1311 du 28 octobre 2009 relative à la protection pénale de la propriété littéraire et artistique sur internet.