Essentiel* de la charte de bon usage du système d'information de l'UPMC

La charte de bon usage définit les règles d'usages et de sécurité du système d'information de l'UPMC, elle précise les droits et devoirs de chacun. Par « *système d'information* » s'entend l'ensemble des moyens matériels, logiciels, applications, bases de données, réseaux de télécommunications et informatique nomade (clé USB, ordinateur portable, téléphone mobile..).

L'UPMC facilite l'accès des utilisateurs au système d'information et met en œuvre toutes les mesures nécessaires pour assurer la sécurité du système d'information et la protection des utilisateurs.

L'utilisateur est responsable, en tout lieu, de l'usage qu'il fait du système d'information auquel il a accès ; il est soumis au respect des obligations résultant de son statut ou de son contrat.

Conditions d'utilisation :

- **Accès au système d'information :** le droit d'accès d'un utilisateur aux ressources informatiques est soumis à autorisation. Ce droit est personnel et incessible. Toute tentative d'accès à des informations détenues par d'autres utilisateurs est considérée comme illicite. Les mots de passe constituent une mesure de sécurité destinée à éviter toute utilisation malveillante ou abusive.
  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, sont des mesures primordiales.

- **Droit d'usage privé résiduel :** l'utilisation résiduelle du système d'information à titre privé est admise sous réserve qu'elle soit licite, non lucrative et raisonnable en termes de fréquence et de durée. 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 ressource de stockage.

- **Continuité de service** : aux seules fins d'assurer la continuité de service, l'utilisateur informe sa hiérarchie des modalités permettant l'accès aux ressources mises spécifiquement à sa disposition.

- **Conformité aux règlements et lois en vigueur :**
  - les logiciels doivent être utilisées dans les conditions des licences souscrites. En l'absence d'autorisation explicite, l' usage de données ou de logiciels protégés par un droit d'auteur est interdit.
  - tout traitement de données nominatives est soumis à déclaration préalable auprès du Correspondant Informatique et Libertés de l'UPMC (cil@upmc.fr).
  - 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.
  - 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.

---

* *Voir la version intégrale de la charte sur l'intranet de l'UPMC à la rubrique : E-Administration > Sécurité systèmes d'information > Textes réglementaires en vigueur à l'UPMC > Charte du bon usage du SI.*

Règles de sécurité applicables :

- **Authentification** : l'utilisateur ne doit pas utiliser son mot de passe « UPMC » pour un usage privé (ie. Connexion sur un site internet grand public). Il doit éviter, par ailleurs, de l'utiliser dans un environnement non sûr (hotspot wifi, cybercafé…). En aucun cas, il ne doit communiquer ce mot de passe à un tiers ; tout courriel demandant lui demandant de fournir un identifiant ou un mot de passe doit être ignoré et, éventuellement, signalé au Responsable de la Sécurité du Système d'Information de l'établissement (rssi@upmc.fr).

- **Utilisation du réseau de l'UPMC :** l'utilisateur s'engage à ne pas connecter aux réseaux locaux des matériels autres que ceux confiés ou autorisés par l'UPMC. L'usage de points d'accès wifi est soumis à réglementation.

- **Protection du patrimoine scientifique :** l'utilisateur s'engage à ne pas déposer des données professionnelles sur un serveur externe et/ou ouvert au grand public (Google, Free, Orange, ...) sans analyse de risques préalable réalisée en concertation avec le Chargé de Sécurité du Système d'Information de l'entité et validée par le directeur de l'unité. Il doit veiller à assurer la protection des informations sensibles de l'unité en évitant de les transporter sans protection (telle qu'un chiffrement) sur des supports mobiles (ordinateurs portables, clés USB, disques externes, etc.).

  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, l'utilisateur doit avertir dans les meilleurs délais le Chargé de Sécurité du Système d'Information de son entité (ou, à défaut, le Responsable de la Sécurité du Système d'Information de l'UPMC). Pour des raisons de maintenance corrective, curative ou évolutive, l'UPMC se réserve la possibilité de réaliser des interventions (le cas échéant à distance) sur les ressources mises la disposition des utilisateurs.

  Les personnels chargés des opérations de maintenance et de contrôle des systèmes d'information sont soumis à l'obligation de discrétion.

- **Messagerie électronique :** l'UPMC 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. La gestion d'adresses électroniques correspondant à des listes de diffusion institutionnelles, désignant une catégorie d'utilisateurs, relève de la responsabilité exclusive de l'UPMC : ces listes ne peuvent être utilisées sans autorisation explicite.

  Tout message est réputé professionnel sauf s'il comporte une mention particulière et explicite (par exemple dans son « Objet ») indiquant son caractère privé ou s'il est stocké dans un espace privé de données. 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.

- **Internet :** tout téléchargement de documents numériques (textes, sons, images, vidéos, etc.) doit s'effectuer dans le respect des lois et règlements en vigueur. Toute publication de pages d'information sur les sites internet ou intranet de l'UPMC doit être validée par un responsable de site ou responsable de publication.

  La mise en œuvre d'un serveur accessible de l'extérieur doit être déclarée à la Direction des Systèmes d'Information, administratrice du réseau, pour en autoriser l'accès. En cas d'incident, l'UPMC se réserve le droit, après information des utilisateurs, de filtrer ou d'interdire l'accès à certains sites, de procéder au contrôle des sites visités.

  Certaines unités, 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 Politique de Sécurité du Système d'Information de ces unités.