The UPMC Information System charter

Acceptable Use Policy: Essentials

The acceptable use policy defines the rules of usage and the security of the UPMC information system. It specifies the rights and duties of each user. "Information system" means all material, software, applications, databases, telecommunications networks and mobile computing (memory stick, laptop, mobile phone ...).

UPMC facilitates user access to the information system and implements all necessary measures to ensure the security of information systems and the protection of the user.

The user is responsible for his use of the information system—regardless of the place of access—and is subject to the obligations resulting from his status or contract.

Terms of Use:

- **Access to the Information System**: The right to a user’s access to computing resources is subject to authorization. This right is personal and not transferable. Any attempt to access information held by others is considered illicit. Passwords are a security measure intended to prevent misuse or abuse.

  Choosing a serious password and changing it if its security is in doubt, especially if it was used from a computer connected to an unsecured external network, are important measures.

- **Right to Residual Privacy**: Residual use of the information system in private is allowed provided it is lawful, non-profit and reasonable in terms of frequency and duration. It is the user’s responsibility to keep his private data in a space created for this purpose by mentioning the private nature of the data on the storage resource.

- **Service Continuity**: For the sole purpose of ensuring the continuity of service, the user will inform his superiors of the access procedures to resources that have been made specifically available to the user.

- **Compliance with applicable laws and regulations**:
  - Software must be used under the conditions of the licenses granted. In the absence of explicit authorization, the use of data or software protected by copyright is forbidden.
  - All processing of personal data is subject to prior declaration to the "Correspondant Informatique et Libertés" (or CIL), the French Data Protection Officer at UPMC (cil@upmc.fr).
  - The right to privacy, images and the right of representation means that no images or information regarding the privacy of others should be put online without prior permission from the person concerned.
  - The use of computer resources made available by UPMC must comply with the RENATER code of ethics. Any commercial use in a private capacity is prohibited.
Safety Requirements:

- **Authentication**: The user should not use his "UPMC" password for private use (i.e. to connect to a website for the general public). He must also avoid using it in an insecure environment (wifi hotspot, internet cafe ...). He must never give this password to a third party; any email that asks him to provide a username or a password should be ignored and then reported to the University’s Chief of IT System Safety (rssi@upmc.fr).

- **Use of the UPMC Network**: The user agrees not to connect to LANs other than those authorized by or entrusted to UPMC. The use of wireless access points is subject to regulation.

- **Protection of Scientific Heritage**: The user agrees not to place professional data on a server that is external and/or open to the public (Google, Free, Orange, ...) without first performing a risk analysis in consultation with the University’s Chief of IT System Safety and obtaining approval from the Director of the unit. The user must ensure the protection of his unit’s sensitive information, particularly avoiding the transportation of data on mobile devices (such as laptops, USB sticks, external drives) unless it is protected (for example, through encryption).

Upon discovery of an abnormality affecting the information system, including intrusion or attempted unauthorized access to a user account, the user must promptly notify the Information System's Safety Officer at the unit (or, failing that, the Information System Security Manager for UPMC). For reasons of corrective, curative or evolutionary maintenance, UPMC reserves the right to intervene (including through remote access) in the resources made available to users.

Those in charge of maintenance and control of information systems are subject to the requirement of discretion.

- **Email**: UPMC is committed to making a user's registered, professional mailbox available to send and receive electronic messages. The use of this registered address is then the responsibility of the user. Management of electronic addresses corresponding to institutional mailing lists, designating a category of users, is the sole responsibility of UPMC: these lists cannot be used without explicit permission.

All messages shall be deemed professional unless they express and special mention (such as a "Subject") line stating its private nature or if stored in a private data space. Electronic messages exchanged with third parties can, legally, form a contract, subject to the conditions laid down in Articles 1369-1 to 1369-11 of the Civil Code.

- **Internet**: any downloading of digital documents (texts, sounds, images, videos, etc.) should be conducted in compliance with laws and regulations. Any publication of pages of information on UPMC websites or intranets must be validated by a site manager or release manager.

The implementation of a server accessible from outside the structure must be reported to the Information Systems Department, with a request for the Network Administrator to authorize access. In the case of a security incident, UPMC reserves the right, after informing the user, to filter or block access to certain sites following an inspection of the sites visited.

Some units, including joint research units, may impose access restrictions due to a higher level of security or a defense classification; specific rules are then in the Information System Security Policy of units.