Charte informatique

Préambule

La présente charte a pour objet de définir les règles d’utilisation des moyens informatiques et numériques mis à disposition des personnels, chercheurs, doctorants, étudiants et invités de l’IMEV.
Elle s’inscrit dans le cadre des réglementations nationales (Code du travail, Code pénal, RGPD) et des politiques de sécurité définies par Sorbonne Université et le CNRS.
Tout utilisateur s’engage à respecter les principes énoncés ci-dessous, afin de garantir la sécurité, l’intégrité et la disponibilité des systèmes d’information, au service de la recherche et de l’enseignement.

---

1. Champ d’application

Cette charte s’applique à l’ensemble des utilisateurs :

- personnels permanents (chercheurs, enseignants-chercheurs, ITA, BIATSS),
- doctorants, post-doctorants, stagiaires,
- étudiants accueillis à l’IMEV,
- personnels invités ou collaborateurs externes disposant d’un accès temporaire.

Elle couvre tous les équipements et services numériques : postes de travail, serveurs, équipements réseaux, messagerie électronique, applications métiers, stockage et traitement des données, accès Internet, ainsi que tout autre outil géré par le Service Informatique et Réseaux (SIR).

---

2. Principes généraux

- Les moyens informatiques sont fournis à des fins professionnelles, pédagogiques ou scientifiques.
- Leur usage doit être conforme aux missions de l’IMEV et ne doit pas porter atteinte à son image, son bon fonctionnement ou à la sécurité des infrastructures.

- Un usage personnel limité et raisonnable est toléré, dans la mesure où il ne nuit ni à l’activité professionnelle ni aux ressources du service.

---

3. Identité numérique et authentification

- Chaque utilisateur dispose d’un compte personnel et nominatif.
- Les identifiants et mots de passe sont strictement personnels et ne doivent jamais être communiqués.
- Les utilisateurs doivent choisir des mots de passe robustes.
- L’accès frauduleux au compte d’autrui est interdit.

---

4. Messagerie électronique et communication

- La messagerie IMEV (Partage de RENATER) est un outil professionnel.
- Les utilisateurs s’engagent à un usage respectueux et conforme à la législation (pas de spam, contenus illicites ou diffamatoires).
- Les pièces jointes volumineuses doivent être transmises via les services sécurisés mis à disposition (FileSender RENATER, sDrive, DropSU).

---

5. Utilisation d’Internet et des réseaux

- L’accès Internet est fourni dans le cadre des missions de recherche, d’enseignement et d’administration.
- Les usages contraires à la loi (téléchargements illégaux, diffusion de contenus illicites, piratage, atteinte aux droits d’auteur, etc.) sont strictement interdits.
- Les utilisateurs doivent respecter les politiques de sécurité du réseau.
- L’installation de bornes Wi-Fi, routeurs ou tout autre équipement réseau non autorisé est interdite.

6. Matériel informatique et logiciels

- Les équipements informatiques (postes de travail, ordinateurs portables, périphériques) doivent être utilisés conformément à leur destination professionnelle. Ces matériels sont la propriété de Sorbonne Université et/ou du CNRS. À ce titre, ils doivent être conservés en bon état et restitués obligatoirement à la fin du contrat ou en cas de départ de l'établissement.
- L'installation de logiciels est soumise à l'autorisation du SIR et doit respecter les règles de licences et de propriété intellectuelle.
- Tout dysfonctionnement ou incident doit être signalé immédiatement au SIR.

7. Données et sauvegardes

- Les utilisateurs doivent stocker leurs données de travail sur les espaces prévus à cet effet (serveurs de l'IMEV, sDrive ou DropSU).
- Les données sensibles (scientifiques, personnelles, administratives) doivent être protégées et ne peuvent être transférées sur des supports non sécurisés sans autorisation.
- Les sauvegardes sur les ressources communes sont assurées par le SIR, mais chaque utilisateur reste responsable de la bonne organisation de ses données.

8. Cybersécurité et protection des systèmes

- Les utilisateurs s'engagent à utiliser l'antivirus préconisé à appliquer les mises à jour de sécurité demandées par le SIR.
- L'usage de logiciels ou dispositifs visant à contourner les protections (antivirus, firewall, filtrage) est interdit.
- Toute suspicion d'incident de sécurité (phishing, virus, intrusion) doit être signalée immédiatement.

9. Données personnelles et confidentialité

- L’IMEV respecte le Règlement Général sur la Protection des Données (RGPD).
- Les utilisateurs doivent protéger les informations confidentielles (scientifiques, administratives, personnelles).

---

10. Responsabilités et sanctions

- Tout utilisateur est responsable de l’usage de son compte et de son poste.
- En cas de non-respect de la charte, des mesures disciplinaires pourront être prises (restriction d’accès, sanctions administratives ou pénales).
- En cas de doute, les utilisateurs doivent se rapprocher du SIR.

---

11. Engagement de l’utilisateur

Tout utilisateur des systèmes d’information de l’IMEV s’engage à respecter la présente charte. L’ouverture et le maintien d’un accès aux ressources numériques est dépendant de l'accord à cette charte informatique.

Revision #6
Created 15 September 2025 08:37:55 by Nicolas Champeil
Updated 2 April 2026 09:40:25 by Nicolas Champeil