PSSIe

Politique de Sécurité des Systèmes d’Information

(PSSI)

Institut de la Mer de Villefranche (IMEV)

La présente Politique de Sécurité des Systèmes d’Information (PSSI) définit les principes, règles et mesures visant à assurer la sécurité des systèmes d’information de l’Institut de la Mer de Villefranche (IMEV).

Elle s’inscrit dans un contexte de coopération renforcée avec Sorbonne Université, le CNRS, Université Côte d’Azur et RENATER, afin de garantir la disponibilité, l’intégrité, la confidentialité et la traçabilité des données et infrastructures numériques nécessaires aux missions scientifiques, administratives et techniques de l’établissement.

1. Objet et périmètre

- La PSSI s’applique à l’ensemble des personnels, chercheurs, enseignants-chercheurs, doctorants, stagiaires, prestataires et partenaires accédant aux ressources numériques de l’IMEV.
- Le périmètre couvre les infrastructures systèmes et réseaux, les serveurs physiques et virtualisés, les équipements scientifiques connectés, les postes de travail, les données scientifiques et administratives, ainsi que les services mutualisés avec les tutelles.

2. Gouvernance de la sécurité

- Le Responsable du Service Informatique et Réseaux (SIR) pilote la mise en œuvre de la PSSI et coordonne les actions de sécurité.
- La Direction valide les orientations stratégiques et les utilisateurs sont responsables du respect des règles d’usage.

3. Principes généraux de sécurité

- Principe du moindre privilège.
- Défense en profondeur.
- Maintien en condition opérationnelle et de sécurité.
- Traçabilité des actions et amélioration continue.

4. Gestion des identités et des accès

- Les accès sont nominatifs et soumis à authentification.
- Les comptes partagés sont interdits.
- L’authentification multifacteur est privilégiée lorsque possible.

5. Sécurité des infrastructures

- Segmentation réseau, filtrage des flux et supervision des équipements.
- Mises à jour régulières, durcissement des configurations et sauvegardes.
- Protection antivirus centralisée et journalisation des événements.

6. Sécurité des postes de travail

- Déploiement automatisé des configurations.
- Installation contrôlée des logiciels.
- Verrouillage automatique des sessions et protection antivirus.

7. Protection des données

- Les données sont classifiées selon leur niveau de sensibilité.
- Les données scientifiques non publiées font l’objet d’une protection renforcée.

8. Continuité et reprise d’activité

- L’IMEV met en œuvre des sauvegardes régulières, des mécanismes de redondance et des procédures de reprise d’activité.
- Les tests de restauration sont réalisés périodiquement.

9. Gestion des incidents de sécurité

- Tout incident doit être signalé au Service Informatique et Réseaux.
- Le SIR coordonne l’analyse, le confinement et la remédiation.

10. Sensibilisation et formation

- Des actions régulières de sensibilisation aux risques cyber sont organisées auprès des utilisateurs.

Revision #1
Created 25 July 2025 15:07:12 by Nicolas Champeil
Updated 25 June 2026 09:35:38 by Nicolas Champeil