Politique de sécurité du système d'information

1. Préambule

L'Institut de la Mer de Villefranche (IMEV) est une fédération de recherche placée sous les tutelles de Sorbonne Université et du CNRS, en partenariat étroit avec Université Côte d’Azur et RENATER.

L’IMEV met à disposition de la communauté scientifique des infrastructures numériques, des plateformes technologiques et des services indispensables aux activités de recherche, d’observation, de formation et de diffusion des connaissances.

L’évolution des usages numériques, le développement de la Science Ouverte, l’accroissement des collaborations nationales et internationales ainsi que l’augmentation constante des menaces cyber rendent nécessaire la mise en œuvre d’une politique de sécurité adaptée aux spécificités de l’établissement.

La présente Politique de Sécurité des Systèmes d’Information d’Établissement (PSSIE) définit les principes de gouvernance, les règles générales et les responsabilités permettant de protéger le système d’information de l’IMEV.

Elle s’inscrit dans le cadre :

- des orientations SSI des tutelles ;
- des recommandations nationales de l’ANSSI ;
- des exigences issues de la réglementation européenne, notamment la directive NIS2.

Elle poursuit les objectifs suivants :

- garantir la disponibilité des services numériques ;
- préserver l’intégrité des données scientifiques et administratives ;
- assurer la confidentialité des informations sensibles ;
- maintenir la continuité des activités scientifiques et administratives ;
- renforcer la résilience face aux cybermenaces.

La sécurité du système d’information constitue une responsabilité collective impliquant la Direction, le Service Informatique et Réseaux (SIR), les responsables de services, les chercheurs,

les personnels administratifs, les étudiants, les partenaires et les prestataires.

---

2. Objet et périmètre

Cette politique définit les principes de sécurité applicables à l’ensemble du système d’information de l’IMEV.

Elle s’applique à toute personne utilisant les ressources numériques de l’établissement, quel que soit son statut :

- personnels permanents ;
- personnels temporaires ;
- étudiants ;
- collaborateurs extérieurs ;
- prestataires.

Le périmètre comprend notamment :

- les infrastructures réseaux ;
- les serveurs physiques et virtualisés ;
- les infrastructures de stockage ;
- les équipements scientifiques connectés ;
- les postes de travail ;
- les équipements mobiles ;
- les services numériques internes ;
- les applications métiers ;
- les plateformes collaboratives ;
- les services mutualisés avec les tutelles ;
- les données scientifiques, administratives et techniques.

Les prestataires et partenaires disposant d’un accès au système d’information sont également soumis aux exigences adaptées de cette politique.

---

3. Gouvernance de la sécurité

3.1 Responsabilité de la Direction

La Direction de l’IMEV :

- valide la présente politique ;
- définit les orientations stratégiques ;
- arbitre les risques acceptés ;
- veille à l’adéquation entre les exigences SSI et les moyens disponibles.

La sécurité des systèmes d’information relève d’une responsabilité institutionnelle et ne peut être portée uniquement par le service informatique.

3.2 Rôle du CSSI

Le CSSI :

- conseille la Direction ;
- accompagne la mise en conformité SSI ;
- assure le relais avec les RSSI des tutelles ;
- participe à l’analyse des risques ;
- contribue à la sensibilisation des utilisateurs.

Le CSSI n’est pas décisionnaire des choix métiers, organisationnels ou budgétaires.

La maîtrise des risques SSI relève de la Direction et des responsables des activités concernées.

3.3 Rôle du SIR

Le Service Informatique et Réseaux assure la mise en œuvre opérationnelle des mesures de sécurité :

- administration des infrastructures ;
- maintien en condition opérationnelle et de sécurité ;
- supervision ;
- gestion des incidents ;
- sauvegarde et restauration ;
- mise en œuvre des mesures techniques.

4. Gestion des risques SSI

L’IMEV adopte une approche fondée sur l’analyse des risques.

Cette démarche vise à identifier :

- les actifs critiques ;
- les menaces ;
- les impacts potentiels ;
- les mesures de protection nécessaires.

Les risques sont évalués selon :

- leur probabilité ;
- leur impact ;
- les mesures existantes ;
- le niveau de risque résiduel.

Les arbitrages liés aux risques acceptés relèvent de la Direction.

---

5. Gestion des actifs numériques

L’IMEV maintient un inventaire des ressources numériques nécessaires à son fonctionnement.

Cet inventaire comprend notamment :

- serveurs ;
- équipements réseau ;
- stockage ;
- applications ;
- services numériques ;
- équipements scientifiques connectés.

Les actifs critiques disposent :

- d’un responsable identifié ;
- d’une classification ;
- d’un niveau de protection adapté ;
- d’un dispositif de sauvegarde ;
- d’un suivi de sécurité.

---

6. Principes fondamentaux de sécurité

La politique SSI repose sur les principes suivants :

- confidentialité ;
- intégrité ;
- disponibilité ;
- authentification ;
- traçabilité ;
- moindre privilège ;
- défense en profondeur ;
- séparation des responsabilités ;
- amélioration continue.

Toute évolution du système d’information doit intégrer la sécurité dès sa conception (« Security by Design »).

---

7. Gestion des identités et des accès

Chaque utilisateur dispose d’un compte nominatif.

Les principes appliqués sont :

- interdiction des comptes partagés sauf justification exceptionnelle ;
- attribution des droits selon le principe du moindre privilège ;

- revue régulière des habilitations ;
- suppression des comptes lors des départs.

Les comptes administrateurs doivent :

- être nominatifs ;
- être limités aux personnes habilitées ;
- être utilisés uniquement pour les opérations nécessitant des privilèges élevés.

L’authentification multifacteur est privilégiée pour :

- les accès distants ;
- les comptes sensibles ;
- les accès administrateurs.

---

8. Sécurité des infrastructures

Le SIR met en œuvre les mesures nécessaires :

- segmentation réseau ;
- filtrage des flux ;
- protection périmétrique ;
- supervision ;
- mises à jour de sécurité ;
- durcissement des configurations ;
- protection antivirale ;
- sauvegardes ;
- journalisation.

Les infrastructures critiques font l’objet d’une surveillance renforcée.

---

9. Sécurité des postes de travail

Les postes utilisateurs doivent être administrés de manière homogène.

Les mesures comprennent :

- déploiement maîtrisé des systèmes ;
- installation contrôlée des logiciels ;
- mises à jour régulières ;
- protection antimalware ;
- verrouillage automatique ;
- limitation des droits administrateurs ;
- chiffrement lorsque nécessaire ;
- inventaire du parc.

Les équipements scientifiques pouvant présenter des contraintes particulières peuvent bénéficier de mesures compensatoires :

- cloisonnement réseau ;
- limitation des accès ;
- supervision renforcée.

---

10. Protection des données

Les données hébergées ou produites par l’IMEV sont classifiées selon leur sensibilité.

Une attention particulière est portée :

- aux données scientifiques non publiées ;
- aux données personnelles ;
- aux données administratives ;
- aux données techniques.

Les accès sont limités aux personnes habilitées.

Les données critiques disposent de mécanismes adaptés de sauvegarde et de restauration.

11. Science Ouverte et données de recherche

L’IMEV applique les principes de la Science Ouverte tout en assurant la protection des données.

Les données de recherche doivent respecter les principes FAIR :

- faciles à trouver ;
- accessibles ;
- interopérables ;
- réutilisables.

Les données sensibles ou confidentielles ne peuvent être diffusées sans validation des responsables concernés.

---

12. Services numériques externes et fournisseurs

Toute utilisation d’un service numérique externe doit faire l’objet d’une évaluation préalable.

Cette analyse prend en compte :

- la nature des données traitées ;
- la localisation des données ;
- les garanties contractuelles ;
- la sécurité proposée ;
- les possibilités de réversibilité.

Cette règle concerne notamment :

- services cloud ;
- solutions SaaS ;
- outils collaboratifs ;

- plateformes d’intelligence artificielle ;
- prestataires techniques.

---

13. Gestion des vulnérabilités

Le SIR assure une veille sur les vulnérabilités affectant les composants du système d’information.

Les actions comprennent :

- application des correctifs ;
- suivi des versions ;
- retrait des systèmes obsolètes ;
- mise en place de mesures compensatoires.

---

14. Continuité d’activité et sauvegarde

Le SI doit garantir un niveau de disponibilité compatible avec les missions de l’établissement.

Le SIR met en œuvre :

- une politique de sauvegarde ;
- des procédures de restauration ;
- des mécanismes de réplication ;
- des tests réguliers.

Les services critiques font l’objet d’une analyse spécifique :

- annuaire ;
- DNS ;
- stockage ;
- virtualisation ;

- sauvegarde ;
- applications scientifiques.

---

15. Gestion des incidents de sécurité

Tout incident de sécurité doit être signalé au SIR.

Le traitement comprend :

- analyse ;
- qualification ;
- confinement ;
- remédiation ;
- restauration ;
- retour d’expérience.

Pour les incidents majeurs, une organisation de crise peut être activée avec :

- Direction ;
- CSSI ;
- SIR ;
- tutelles concernées.

---

16. Journalisation et supervision

Les systèmes critiques font l’objet d’une collecte adaptée des événements de sécurité.

Les objectifs sont :

- détecter les comportements suspects ;
- faciliter les investigations ;

- assurer la traçabilité.

---

17. Sensibilisation des utilisateurs

Des actions régulières sont organisées concernant :

- phishing ;
- mots de passe ;
- protection des données ;
- usages numériques ;
- télétravail.

Chaque utilisateur doit respecter la charte informatique.

---

18. Contrôle et amélioration continue

La conformité à la présente politique peut faire l’objet :

- d’audits ;
- de contrôles ;
- de revues régulières.

Les incidents, évolutions technologiques et nouvelles menaces alimentent une démarche d’amélioration continue.

Des indicateurs SSI peuvent être suivis :

- état des sauvegardes ;
- incidents ;
- vulnérabilités ;
- mises à jour ;

- comptes actifs ;
- actions de sensibilisation.

---

19. Révision de la PSSIE

La présente PSSIE est révisée :

- au minimum tous les trois ans ;
- lors d’une évolution majeure du SI ;
- lors d’une évolution réglementaire significative.

Toute modification est soumise à validation de la Direction.

Documents associés

- Charte informatique utilisateur ;
- Politique de gestion des comptes ;
- Politique de sauvegarde ;
- Procédure de gestion des incidents ;
- Plan de reprise d’activité ;
- Inventaire des actifs ;
- Analyse de risques SSI.

Revision #10
Created 2023-09-15 15:24:21 UTC by Nicolas Champeil
Updated 2026-08-07 12:08:23 UTC by Nicolas Champeil