Politique de sécurité du système d'information

Le principe de base concernant les ressources informatiques est que leur usage doit respecter la législation (droit d’auteur, pas de contournement des moyens de sécurité, aucune intrusion interne ou externe sur des systèmes informatiques sur lequel on ne dispose pas de droits d’accès, pas d’incitation à la haine raciale, etc.) et le règlement intérieur de l'IMEV.

Tout utilisateur de l'IMEV est soumis aux chartes de bonnes utilisations suivantes

- Charte générale à l'usage des ressources numériques
- Cadre national ANSSI, PSSIE

Table des matières

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. Il met à disposition de la communauté scientifique des infrastructures numériques, des plateformes technologiques et des équipements scientifiques 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, la multiplication des collaborations internationales et l'augmentation des menaces cyber rendent indispensable la mise en œuvre d'une politique de sécurité cohérente, adaptée aux spécificités de l'IMEV.

La présente Politique de Sécurité des Systèmes d'Information (PSSI) fixe les principes de gouvernance et les règles générales destinées à protéger les systèmes d'information de l'établissement.

Elle poursuit cinq objectifs :

- 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 de recherche et de support ;
- répondre aux exigences réglementaires et aux engagements des tutelles.

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.

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, qu'elle soit permanente ou temporaire.

Le périmètre comprend notamment :

- les infrastructures réseaux ;
- les serveurs physiques et virtualisés ;
- les équipements de stockage ;
- les postes de travail ;
- les équipements mobiles ;
- les équipements scientifiques connectés ;
- les services numériques internes ;
- les applications métiers ;

- les plateformes collaboratives ;
- les services mutualisés avec les tutelles ;
- les données scientifiques, administratives et techniques.

Les exigences de cette politique s'appliquent également aux prestataires et partenaires disposant d'un accès au système d'information.

Contexte et enjeux

Le système d'information de l'IMEV constitue un outil essentiel au fonctionnement de l'établissement. Il soutient les activités de recherche, les plateformes technologiques, les observatoires, les services administratifs ainsi que les collaborations nationales et internationales.

Les principaux enjeux sont :

- protéger les données scientifiques avant leur publication ;
- garantir l'accès aux plateformes numériques ;
- sécuriser les équipements scientifiques connectés ;
- préserver les données administratives et financières ;
- assurer la disponibilité des infrastructures ;
- favoriser la diffusion des données conformément aux principes de la Science Ouverte tout en maîtrisant les risques.

Gouvernance de la sécurité

La Direction définit les orientations stratégiques et valide la présente politique.

Le Service Informatique et Réseaux est responsable de sa mise en œuvre opérationnelle. Il assure notamment l'administration des infrastructures, le maintien en condition de sécurité, la supervision des systèmes, la gestion des incidents et la mise en œuvre des mesures techniques de protection.

Chaque utilisateur est responsable du respect des règles définies dans la présente politique et dans la Charte informatique.

Les responsables de services et de plateformes veillent à l'application des mesures de sécurité dans leur domaine d'activité.

Principes fondamentaux

La politique de sécurité repose sur les principes suivants :

- confidentialité des informations ;
- intégrité des données ;
- disponibilité des services ;
- authentification des utilisateurs ;
- traçabilité des actions ;
- principe du 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 »).

Gestion des identités et des accès

Chaque utilisateur dispose d'un compte nominatif.

- Les comptes partagés sont interdits, sauf justification technique exceptionnelle validée par le SIR.
- Les droits sont attribués selon le principe du moindre privilège et revus régulièrement.
- L'authentification multifacteur est privilégiée pour les accès sensibles ou distants.
- Les comptes sont créés, modifiés et supprimés selon une procédure formalisée.

Sécurité des infrastructures

Le Service Informatique et Réseaux met en œuvre les mesures nécessaires pour assurer la sécurité des infrastructures :

- segmentation des réseaux ;
- filtrage des flux ;
- supervision permanente ;
- mises à jour régulières ;
- durcissement des configurations ;
- protection antivirus centralisée ;
- sauvegardes ;
- journalisation des événements.

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

Sécurité des postes de travail

Les postes de travail constituent le principal point d'entrée vers le système d'information de l'IMEV. Ils doivent être administrés de manière homogène afin de garantir un niveau de sécurité conforme aux exigences de l'établissement.

Le Service Informatique et Réseaux met en œuvre des solutions permettant d'assurer le maintien en condition opérationnelle et de sécurité des équipements informatiques.

Les mesures suivantes sont appliquées :

- déploiement automatisé des systèmes d'exploitation et des configurations de sécurité ;
- installation des logiciels selon une procédure maîtrisée et validée par le Service Informatique et Réseaux ;
- application régulière des mises à jour de sécurité des systèmes d'exploitation et des applications ;
- protection antivirus et antimalware centralisée sur les postes compatibles ;
- activation du pare-feu local lorsque cela est applicable ;
- verrouillage automatique des sessions après une période d'inactivité ;
- limitation des privilèges administrateurs aux seules personnes habilitées ;
- chiffrement des postes portables et des équipements mobiles contenant des données sensibles, lorsque cela est techniquement possible ;
- inventaire et suivi du parc informatique ;
- remplacement ou retrait des équipements devenus obsolètes ou ne bénéficiant plus d'un support de sécurité.

Les utilisateurs ne doivent pas installer de logiciels sans l'accord du Service Informatique et Réseaux, désactiver les mécanismes de sécurité ou modifier les configurations susceptibles de compromettre la sécurité du poste ou du système d'information.

Les postes pilotant des équipements scientifiques peuvent faire l'objet de mesures spécifiques lorsque les contraintes des constructeurs ou des logiciels d'acquisition ne permettent pas l'application complète des politiques de sécurité. Dans ce cas, des mesures compensatoires, telles que le cloisonnement réseau, la limitation des accès ou le renforcement de la supervision, sont mises en œuvre.

Protection des données

Les données produites ou hébergées 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 relatives aux infrastructures.

Les données critiques sont sauvegardées régulièrement et leur accès est limité aux personnes habilitées.

Science Ouverte et gestion des données de la recherche

L'IMEV s'inscrit pleinement dans la politique nationale de Science Ouverte.

Les données de recherche doivent être gérées conformément aux principes FAIR (Faciles à trouver, Accessibles, Interopérables et Réutilisables), tout en tenant compte des exigences de confidentialité, des contraintes réglementaires et des engagements contractuels.

Lorsque cela est possible, les jeux de données sont accompagnés de métadonnées de qualité et publiés dans des entrepôts ou catalogues adaptés, avec une licence précisant leurs conditions de réutilisation.

Les données sensibles, confidentielles ou soumises à des restrictions ne sont diffusées qu'après validation des responsables scientifiques et administratifs.

Continuité d'activité et sauvegardes

Le système d'information 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 et un plan de reprise d'activité adaptés à la criticité des services.

Des tests réguliers sont réalisés afin de vérifier l'efficacité des dispositifs de restauration.

Gestion des incidents

Tout incident de sécurité doit être signalé sans délai au Service Informatique et Réseaux.

Le SIR assure :

- l'analyse ;
- le confinement ;
- la remédiation ;
- la restauration des services ;
- le retour d'expérience.

Les incidents majeurs sont portés à la connaissance de la Direction et, si nécessaire, des tutelles.

Sensibilisation des utilisateurs

La sécurité repose également sur les comportements des utilisateurs.

Des actions régulières de sensibilisation sont organisées concernant :

- les risques liés au phishing ;
- les mots de passe ;
- la protection des données ;
- les usages en télétravail ;
- les bonnes pratiques numériques.

Chaque utilisateur est tenu de respecter la Charte informatique.

Contrôle et amélioration continue

Le respect de la présente politique peut faire l'objet de contrôles, d'audits ou de revues de conformité.

Les incidents, les évolutions technologiques, les retours d'expérience et les nouvelles menaces alimentent une démarche d'amélioration continue visant à renforcer le niveau global de sécurité.

Révision de la PSSI

La présente PSSI est révisée au minimum tous les trois ans ou à l'occasion d'une évolution significative des infrastructures, de l'organisation ou du contexte réglementaire.

Toute modification est soumise à la validation de la Direction.

Revision #9
Created 15 September 2023 13:24:21 by Nicolas Champeil
Updated 25 June 2026 09:38:22 by Nicolas Champeil