PSSI

- Politique de sécurité du système d'information
- Annexe 1 — Cartographie des actifs critiques du système d’information IMEV
- Annexe 2 — Matrice de criticité NIS2 des actifs IMEV
- Annexe 3 — Analyse des risques SSI IMEV

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.

Annexe 1 — Cartographie des actifs critiques du système d’information IMEV

1. Objectif

Cette cartographie identifie les composants du système d’information dont l’indisponibilité, la compromission ou la perte d’intégrité pourrait avoir un impact significatif sur les activités scientifiques, administratives ou institutionnelles de l’IMEV.

Elle constitue un élément de référence dans :

- l’analyse des risques SSI ;
- la définition des priorités de sécurité ;
- la gestion des incidents ;
- la préparation des plans de continuité et de reprise d’activité.

---

2. Vue globale du système d’information IMEV

3. Inventaire des actifs critiques

Domaine	Actif	Rôle	Criticité	Impact en cas d'arrêt
Identité	Active Directory	Authentification utilisateurs, postes, services	Critique	Blocage global des accès
Identité	OpenLDAP	Services Linux, applications scientifiques	Critique	Perte accès applications
DNS	DNS publics / internes	Résolution services	Critique	Indisponibilité services
Réseau	Pare-feu Palo Alto	Protection périmétrique	Critique	Perte connectivité
Réseau	Commutateurs cœur réseau	Interconnexion bâtiments/services	Critique	Isolement des infrastructures
VPN	GlobalProtect	Accès distant sécurisé	Haute	Perte accès distant
Virtualisation	VxRail	Hébergement serveurs virtuels	Critique	Arrêt services hébergés
Stockage	Dell Unity XT	Stockage centralisé	Critique	Perte accès données
Sauvegarde	Veeam Backup / Acronis	Protection données	Critique	Risque perte définitive
Supervision	Zabbix	Surveillance infrastructure	Haute	Réduction capacité détection
Messagerie	RENATER Partage	Communication institutionnelle	Haute	Impact organisationnel
Collaboration	Nextcloud	Partage fichiers	Haute	Impact utilisateurs
Développement	GitLab	Gestion code/scripts	Moyenne	Impact exploitation
Scientifique	Serveurs de calcul/acquisition	Activités recherche	Haute	Impact scientifique

---

4. Données critiques

Type de données	Exemple	Niveau
Données scientifiques non publiées	Observations, mesures, résultats intermédiaires	Critique

Type de données	Exemple	Niveau
Données issues des plateformes scientifiques	Instruments, capteurs, acquisitions	Critique
Données administratives	Gestion établissement	Haute
Données utilisateurs	Documents personnels professionnels	Haute
Données techniques SI	Configurations, scripts, sauvegardes	Critique
Données publiques	Publications, données ouvertes	Standard

5. Dépendances critiques

Dépendance identité

```
AD / LDAP
    |
    +-- Serveurs Linux
    |
    +-- Applications
    |
    +-- VPN
    |
    +-- Services utilisateurs
```

Dépendance stockage

```
Unity XT
    |
```

```
    +-- Serveurs virtuels
    |
    +-- Données scientifiques
    |
    +-- Partages utilisateurs
```

Dépendance sauvegarde

```
Production
    |
    ↓
Veeam
    |
    ↓
Stockage secondaire
    |
    ↓
Restauration PRA
```

Annexe 2 — Matrice de criticité NIS2 des actifs IMEV

1. Méthode d'évaluation

Chaque actif est évalué selon quatre critères :

Critère	Description
Disponibilité	Impact d'une indisponibilité
Intégrité	Risque de modification ou corruption
Confidentialité	Sensibilité des informations
Traçabilité	Besoin d'audit et investigation

Notation :

Niveau	Signification
1	Faible
2	Modéré
3	Important
4	Critique

---

2. Matrice de criticité

Actif	Disponibilité	Intégrité	Confidentialité	Criticité globale
Active Directory	4	4	3	Critique
LDAP	4	4	3	Critique
DNS	4	4	2	Critique

Actif	Disponibilité	Intégrité	Confidentialité	Criticité globale
Firewall	4	4	3	Critique
VxRail	4	4	3	Critique
Unity XT	4	4	4	Critique
Veeam	4	4	4	Critique
VPN	3	4	4	Haute
Messagerie	3	3	3	Haute
Nextcloud	3	3	4	Haute
Serveurs scientifiques	3	4	4	Haute
GitLab	2	3	3	Moyenne
Postes utilisateurs	2	3	3	Moyenne

---

3. Priorisation des mesures de sécurité

Niveau critique

Mesures obligatoires :

- sauvegarde régulière ;
- supervision ;
- journalisation ;
- contrôle d’accès renforcé ;
- MFA si applicable ;
- maintien en condition de sécurité ;
- documentation.

Actifs concernés :

- AD ;
- LDAP ;
- DNS ;

- Unity XT ;
- VxRail ;
- Veeam ;
- Firewall.

Niveau haute

Mesures :

- suivi des mises à jour ;
- contrôle des accès ;
- supervision ;
- sauvegarde adaptée.

Actifs concernés :

- VPN ;
- messagerie ;
- Nextcloud ;
- serveurs scientifiques.

Niveau moyenne

Mesures :

- gestion standard ;
- mise à jour régulière ;
- protection poste.

Actifs concernés :

- postes utilisateurs ;
- services secondaires.

---

4. Correspondance avec les exigences NIS2

Exigence NIS2	Réponse IMEV
Gestion des risques	Analyse de criticité des actifs
Sécurité des infrastructures	Architecture réseau segmentée
Gestion des accès	AD / LDAP / MFA
Continuité activité	Sauvegarde Veeam et Acronis + PRA
Gestion incidents	Procédure SSI
Sécurité fournisseurs	Évaluation services externes
Protection données	Classification données
Amélioration continue	Revue annuelle SSI

---

5. Évolution attendue

Cette cartographie doit être maintenue :

- au minimum annuellement ;
- lors de l’arrivée d’un nouveau service critique ;
- lors d’une évolution majeure d’infrastructure ;
- après un incident significatif.

Responsables :

- SIR : mise à jour technique ;
- CSSI : suivi SSI ;
- Direction : validation des risques.

Annexe 3 — Analyse des risques SSI IMEV

Méthode EBIOS simplifiée

Version : 1.0
Pilote : CSSI IMEV
Contributeurs : SIR, responsables de plateformes, responsables métiers

---

1. Objectifs

L’analyse des risques SSI vise à :

- identifier les risques pesant sur le système d’information de l’IMEV ;
- évaluer leurs impacts potentiels sur les activités scientifiques et administratives ;
- définir les mesures de sécurité adaptées ;
- prioriser les actions en fonction du niveau de risque.

Cette analyse s’inscrit dans une démarche d’amélioration continue et répond aux principes de gestion des risques attendus dans le cadre de NIS2.

---

2. Méthodologie retenue

La méthode retenue est une adaptation simplifiée de la méthode **EBIOS Risk Manager**.

Elle repose sur :

1. Identification des valeurs métiers ;
2. Identification des actifs supports ;
3. Identification des menaces ;
4. Évaluation des impacts ;

5. Définition des mesures de réduction du risque.

3. Valeurs métiers critiques IMEV

Valeur métier	Description	Criticité
Activités scientifiques	Recherche marine, observation, expérimentation	Critique
Données scientifiques	Mesures, acquisitions, résultats non publiés	Critique
Plateformes technologiques	Moyens numériques et scientifiques mutualisés	Critique
Services numériques	Messagerie, stockage, authentification	Haute
Données administratives	Gestion établissement	Haute
Communication scientifique	Diffusion des résultats	Moyenne

4. Actifs supports critiques

Actif support	Fonction	Criticité
Active Directory	Authentification utilisateurs	Critique
OpenLDAP	Authentification Linux/applications	Critique
DNS	Résolution services	Critique
Pare-feu Palo Alto	Sécurité réseau	Critique
VxRail	Virtualisation	Critique
Dell Unity XT	Stockage centralisé	Critique
Veeam	Sauvegarde/restauration	Critique
VPN GlobalProtect	Accès distant	Haute
Serveurs scientifiques	Applications recherche	Haute

Actif support	Fonction	Criticité
Nextcloud	Collaboration	Haute
Messagerie RENATER	Communication	Haute

---

5. Événements redoutés

ER01 — Indisponibilité du stockage central

Description

Perte d’accès aux données hébergées sur le stockage central.

Impacts

- arrêt de services scientifiques ;
- interruption des utilisateurs ;
- perte de productivité ;
- retard des projets.

Gravité

Critique

ER02 — Compromission d’un compte utilisateur

Description

Utilisation frauduleuse d’un compte légitime.

Impacts

- accès non autorisé aux données ;
- propagation malware ;
- fuite d’informations.

Gravité

Haute

ER03 — Ransomware

Description

Chiffrement des systèmes et données.

Impacts

- arrêt activité ;
- perte disponibilité ;
- restauration longue.

Gravité

Critique

ER04 — Perte d’un service d’identité

Description

Indisponibilité AD/LDAP.

Impacts :

- impossibilité de connexion ;
- arrêt applications ;
- blocage administration.

Gravité :

Critique

ER05 — Fuite de données scientifiques

Description

Divulgation de données avant publication.

Impacts :

- perte d’avantage scientifique ;
- impact réputation ;
- non-respect engagements.

Gravité :

Critique

ER06 — Défaillance matérielle majeure

Description

Panne stockage, serveur ou réseau.

Impacts :

- interruption service ;
- intervention urgente ;
- perte disponibilité.

Gravité :

Haute

---

6. Sources de menace

Menace	Origine possible
Cyberattaque externe	Internet
Phishing	Utilisateurs
Malware/Ransomware	Poste compromis
Erreur humaine	Manipulation utilisateur
Mauvaise configuration	Administration

Menace	Origine possible
Défaillance matériel	Infrastructure
Prestataire compromis	Chaîne fournisseur
Compte privilégié compromis	Administration

---

7. Analyse des risques

Notation :

- Probabilité : 1 à 4
- Impact : 1 à 4

Niveau risque :

Score	Niveau
1-4	Faible
5-8	Modéré
9-12	Important
13-16	Critique

Matrice des risques IMEV

Risque	Probabilité	Impact	Niveau
Ransomware	3	4	Critique
Compromission compte utilisateur	3	3	Important
Panne stockage Unity	2	4	Important
Perte AD/LDAP	2	4	Important
Fuite données scientifiques	2	4	Important
Défaillance serveur critique	2	3	Modéré

Risque	Probabilité	Impact	Niveau
Mauvaise configuration réseau	2	3	Modéré
Compromission fournisseur	2	3	Modéré

---

8. Mesures existantes IMEV

Protection identité

Déjà en place :

- AD
- OpenLDAP
- synchronisation annuaire
- gestion centralisée comptes

À renforcer :

- MFA généralisé ;
- revue droits régulière.

Protection infrastructure

Déjà en place :

- segmentation réseau
- firewall Palo Alto
- virtualisation VxRail
- stockage Unity XT
- sauvegarde Veeam

À renforcer :

- supervision sécurité ;
- analyse logs ;
- durcissement.

Protection données

Déjà en place :

- sauvegarde centralisée
- réplication secondaire
- stockage mutualisé

À renforcer :

- classification données ;
- règles conservation ;
- tests restauration.

9. Plan de traitement des risques

Risque	Action	Priorité
Ransomware	MFA + sensibilisation + sauvegardes immuables	Haute
Compte compromis	MFA + revue droits	Haute
Perte stockage	PRA + tests restauration	Haute
Fuite données	Classification + contrôle accès	Haute
Vulnérabilités	Gestion patchs	Haute
Logs insuffisants	SIEM / centralisation logs	Moyenne
Shadow IT	Processus validation outils	Moyenne

10. Risques résiduels et arbitrages

La réduction totale du risque n’étant pas possible, l’IMEV définit un niveau de risque résiduel acceptable.

Les risques résiduels nécessitant des moyens supplémentaires font l’objet d’un arbitrage de la Direction.

Le SIR assure la mise en œuvre opérationnelle des mesures validées dans la limite des ressources disponibles.

---

11. Gouvernance de suivi

Cette analyse est revue :

- annuellement ;
- lors d’une évolution majeure du SI ;
- après un incident significatif ;
- lors d’un changement réglementaire.

Participants :

- Direction IMEV ;
- CSSI ;
- SIR ;
- responsables métiers concernés.

Conclusion

Cette analyse permet à l’IMEV de disposer d’une vision structurée de ses risques numériques et de prioriser ses actions de sécurité conformément aux principes de NIS2.

Elle constitue également un support d’aide à la décision pour définir les moyens humains, techniques et financiers nécessaires au maintien d’un niveau de sécurité adapté aux missions scientifiques de l’établissement.