Sécurité de l'information

Classification	C2 - Interne
Référence	POL-001
Propriétaire	Président
Statut	En vigueur
Prochaine revue	10/02/2029
Version	V2
Date de la version	10/02/2026

Historique des modifications

Version	Rédacteur(s)	Approbateur
V2 du 10/02/2026	**Rania Horrigue (Responsable Qualité) Thierry Despres (Président)**	**Thierry Despres (Président)**
	Modification du paragraphe 6.3 (Communication) : La politique est communiquée aux parties intéressées externes seulement sur demande.	
V1 du 26/11/2025	Rania Horrigue (Responsable Qualité) Thierry Despres (Président)	Thierry Despres (Président)

1: Objectif

La présente politique fait partie du Framework cybersécurité de ISKernel. Son objectif est de définir La stratégie, l'organisation, les objectifs et l'engagement en matière de protection de la sécurité de l'information.

2: Scope

Cette politique s’applique à l’ensemble du personnel, collaborateurs et partenaires impliqués dans le traitement de l’information au sein de ISKernel.

3: Engagement de la direction

La direction s'engage à :
• Allouer les ressources nécessaires pour la mise en place d’un SMSI.
• Satisfaire toutes les exigences applicables en matière de sécurité de l’information.
• Améliorer en continue le SMSI

4: Glossaire

Ce paragraphe est dédié à l’explication des notions marquées par un Astérix (*) au niveau des règles et recommandations.

- SMSI : Système de Management de la Sécurité de l'Information
- PSI : Politique de la sécurité de l’information
- SI : Système d'information

5: Revue

La présente politique doit être mise à jour tous les 3 ans et en cas de modifications majeures des pratiques relatives à la stratégie et l’organisation.

6: Enoncé de la politique

6.1: Objectifs de la sécurité de l'information

Les objectifs à atteindre de notre système de management de la sécurité de l'information sont les suivants :
• OBJ-1 : Assurer la protection de la confidentialité, de l'intégrité et de la disponibilité de nos données ainsi que des données personnelles et de santé de nos clients ;
• OBJ-2 : Renforcer la sensibilisation du personnel à la sécurité de l'information et aux politiques internes pour assurer leur conformité et engagement ;
• OBJ-3 : Renforcer la posture de sécurité et la résilience face aux attaques.;
• OBJ-4 : Aligner la sécurité de l'information aux objectifs de ISKernel ;
• OBJ-5 : Être conforme aux normes et réglementations internationales et locales (ISO 27001, HDS, RGPD) ;
Les objectifs peuvent être réajustés en fonction de la stratégie de l'entreprise et seront accompagnés d'indicateurs de performance permettant d'évaluer leur réalisation.

6.2: Stratégie

L'atteinte de ces objectifs passera par notre stratégie qui gravite autour des éléments suivants :

APPROCHE PAR LES RISQUES

L'approche par les risques permet d'adopter une démarche pragmatique. En effet, la prise de décision doit se faire en connaissance des risques de sécurité. Cette approche permet de mettre en place des mesures de sécurité appropriées et adaptées dans toutes les circonstances. Ainsi chaque prise de décision doit s'accompagner d'une étude des risques de sécurité, à l'instar des études des risques financiers, d'image ou juridiques.

DÉFENSE EN PROFONDEUR

La défense en profondeur implique l'utilisation de multiples couches de défenses stratégiquement positionnées pour protéger le Système d'Information et les données contre les cybermenaces. Cette approche vise à rendre plus difficile pour les attaquants la compromission d'un système en reliant les pares-feux de sécurité telles que les pares-feux, les systèmes de détection d'intrusion, la gestion des identités et des accès, le chiffrement des données, la surveillance réseau et la formation des utilisateurs

L'INTÉGRATION DE LA SÉCURITÉ DANS LES PROJETS

Chaque projet utilisant des systèmes d'information (de ISKernel ou de tiers) doit faire l'objet d'une étude de sécurité dès le début du projet. Cette étude vise à identifier, évaluer, cartographier et partager les risques de sécurité liés au projet afin d'identifier les mesures de sécurité à mettre en place pour traiter les risques. Les mesures de sécurité identifiées doivent être intégrées dans les conceptions générales, techniques et détaillées du projet et elles doivent être mises en place avant la mise en production.

PROTECTION DES ACTIFS

La protection des actifs vise à sécuriser les ressources critiques de ISKernel contre diverses menaces et vulnérabilités. Les actifs peuvent comprendre des données, le personnel, les processus, les applications, l'infrastructure etc. En renforçant la protection des actifs, on minimise les risques et on améliore la résilience globale face aux menaces et aux attaques cybernétiques.

PROTECTION DES SYSTÈMES ET RÉSEAUX

Elle implique la mise en place de mesures de sécurité robustes pour prévenir les cyberattaques,

détecter les activités malveillantes et réagir efficacement aux incidents. La surveillance continue du réseau et des systèmes est essentielle pour détecter toute activité suspecte ou intrusion potentielle ou de considérer les réseaux difficilement sécurisables comme un réseau public vecteur d'attaque hostike

GESTION DES CORRECTIFS ET DES VULNÉRABILITÉS

La gestion de l'obsolescence et des correctifs de sécurité est un enjeu majeur dans la gestion de la sécurité du SI*. De par la multiplicité des systèmes et technologies composant le SI et de par la recrudescence des attaques de grande ampleur, il est important que les systèmes soient à jour et protégés contre toute exploitation malveillante. C'est d'autant plus important sur les systèmes supportant des services, applications ou données sensibles.

SENSIBILISATION

Les initiatives de sensibilisation aux risques en matière de sécurité de l'information auprès des collaborateurs doivent être renforcées. Une campagne de sensibilisation annuelle doit être organisée. La sensibilisation doit notamment être effectuée sur des thématiques adaptées aux métiers de chacun et proche de leur quotidien.

CYBER RÉSILIENCE

Le renforcement de la réglementation européenne, qui est applicable depuis le 25 mai 2018, concernant la protection des données personnelles, et les droits des individus concernant leurs données, contraint ISkernel à la mise en place de mesure de sécurité permettant de se mettre en conformité. Ces actions de mise en conformité sont transverses et nécessitent l'attention de chacun dans la mesure où la non-conformité à la réglementation pourrait conduire à une très forte amende financière.

GESTION DES ACCÈS LOGIQUES

La gestion des accès logiques est un point clé dans la gestion de la sécurité du SI* de ISKernel. De part sa complexité, les accès logiques permettent de contrôler l'usage des ressources informatiques en accord avec les besoins de chaque population et avec la politique d'accès.

GESTION DES FOURNISSEURS

L'intégration de la sécurité dans les contrats avec les tiers est également un chantier majeur pour que la présente PSI* s'applique également à ces derniers et que les mesures de sécurité soient adaptées à chaque type de prestation de service, notamment les fournisseurs de services (solutions logicielles, externalisation), les partenaires avec lesquels des informations sont transférées / reçues, ou encore les hébergeurs.

AMÉLIORATION CONTINUE

Le reporting des sujets de sécurité permet de construire et de piloter la démarche d'amélioration continue de la sécurité. Ce reporting permet également de coordonner les projets et les mesures de sécurité tout en apportant les informations nécessaires à la prise des décisions d'entreprise en connaissant les enjeux de sécurité.

6.3: Communication

• La PSI* doit être communiquée au sein de l'entreprise. Cette politique est disponible sur notre interface de gestion documentaire Hermès sous la référence POL-001.
• La PSI* peut être transmise aux parties intéressées sur demande.

6.4: Respect de la politique

• Chaque employé doit protéger l’information mise à sa disposition et à respecter la présente Politique. Le cas échéant des mesures disciplinaires doivent être appliqué par la direction.
• Chaque employé doit signaler au CTO, ou encore à la Direction, sans tarder, tout événement non conforme à la présente Politique.