

L'information constitue aujourd'hui un actif stratégique pour les organisations, évoluant au rythme des innovations technologiques, des nouvelles menaces numériques et des exigences réglementaires. Consciente de ces enjeux, KEYSTONE reconnaît que la sécurité de l'information est essentielle à la pérennité de ses activités et à la confiance durable de ses parties prenantes.

Dans un contexte marqué par la transformation numérique, l'augmentation des risques liés à la cybercriminalité, et l'exigence de conformité à des référentiels nationaux et internationaux, la Direction Générale de KEYSTONE a pris la décision d'établir un **Système de Management de la Sécurité de l'Information (SMSI)** conforme à la norme **ISO/IEC 27001:2022**.

La présente politique vise à encadrer la gouvernance du SMSI et à affirmer l'engagement de KEYSTONE autour des axes suivants :

- **Fournir des services sécurisés et fiables**, répondant durablement aux attentes de ses parties prenantes internes et externes.
- **Assurer la confidentialité, l'intégrité et la disponibilité des informations**, y compris les données à caractère personnel traitées dans le cadre de ses activités.
- **Renforcer les compétences techniques et sécuritaires du personnel**, à travers la sensibilisation, la formation continue et l'implication active de chacun dans le SMSI.
- **Maintenir une infrastructure informatique robuste et résiliente**, adaptée à l'évolution des menaces et garantissant la sécurité des services offerts.
- **Développer un écosystème de confiance**, fondé sur un partenariat renforcé avec les parties prenantes internes et externes (clients, partenaires, autorités...).

Pour atteindre ces objectifs, la Direction Générale de KEYSTONE s'engage à :

- **Traduire les axes stratégiques de cette politique en objectifs mesurables**, suivis dans le cadre du SMSI, et à conduire des revues régulières (au moins annuelles) pour évaluer leur atteinte.
- **Garantir la conformité** des services aux exigences légales, réglementaires et contractuelles, ainsi qu'aux besoins explicites des parties intéressées.
- **Favoriser l'amélioration continue du SMSI** en s'appuyant sur l'analyse des résultats, des incidents, des risques et opportunités, et sur les retours d'expérience.
- **Allouer les ressources humaines, techniques et financières nécessaires** à la mise en œuvre et à l'efficacité du SMSI dans toutes ses dimensions.
- **Intégrer le SMSI dans la gouvernance globale de l'organisation**, en l'alignant sur la stratégie et les valeurs de KEYSTONE.

Le SMSI couvre **l'ensemble des activités du Security Operations Center (SOC)** de KEYSTONE, ainsi que les services associés contribuant à la surveillance, la détection, l'investigation et la réponse aux incidents de sécurité.

La mise en œuvre opérationnelle du SMSI est assurée par le **Responsable Sécurité de l'Information**, sous la coordination du **Comité de sécurité de l'information de KEYSTONE**.

La réussite de cette démarche repose sur **l'implication, la vigilance et la responsabilité collective** de tous les collaborateurs. Chacun est acteur de la sécurité de l'information et contribue à faire de KEYSTONE un partenaire de confiance reconnu pour la **qualité et la sécurité de ses services**.

La Direction Générale
M. Haythem EL MIR

