POLITIQUE DE SÉCURITÉ GÉNÉRALE :

LETTRE D'ENGAGEMENT DU DIRIGEANT

L'actualité témoigne des risques liés à l'évolution des usages numériques : fuite d'informations, perte ou réduction d'activité, atteinte à l'image de marque, exploitation excessive de données personnelles.
Dans le but de protéger nos clients, les utilisateurs de nos services et les parties prenantes (nos salariés, nos partenaires, nos actionnaires) contre ces menaces, nous avons mis en place une entité dédiée à la sécurité du système d'information et un Système de Management de la Sécurité de l'Information (SMSI) sous la responsabilité du RSSI (Responsable de la sécurité du système d'information).
Le SMSI que nous avons déployé fait partie intégrante du système de management déjà en place.
Ainsi, l'ensemble des membres de la direction générale soutient l'équipe chargée de sa mise en œuvre en lui donnant les moyens budgétaires et humains pour effectuer sa mission.
La direction générale s'engage également à suivre l'efficacité du SMSI en orientant et en contrôlant sa performance.

Nous améliorons sans cesse nos méthodes et outils pour :

- protéger notre système d'information,
- accroître notre performance et proposer des solutions fiables répondant à nos attentes et prenant en compte les exigences les plus fortes parmi les normes et réglementations (ISO 27001, règlement relatif à la protection des données à caractère personnel) ainsi que les exigences (traçabilité, transparence ...) de nos clients et autres parties intéressées.

Nous nous appuyons en priorité sur les compétences internes et sollicitons des experts extérieurs chaque fois que cela s'avère nécessaire. Pour chaque actif matériel et immatériel, un examen des menaces associées et vulnérabilités est transposé dans une analyse de risque en prenant en compte l'impact en termes de disponibilité, d'intégrité, de confidentialité et de traçabilité.
Toute évolution portant sur un des composants de notre système d'information englobe une approche et une validation sur la partie « sécurité du système d'information ». Des règles de classification et de protection de l'information sont définies et déployées.
Toute personne accédant à une information est responsable quant à son utilisation et notamment lors du transfert ou de la mise à disposition à un tiers. Elle doit donc respecter les règles édictées dans ce domaine et celles de la charte informatique.

Nous nous engageons, dans une volonté d'amélioration continue, à mettre en œuvre les actions et moyens nécessaires pour :

- obtenir et maintenir la certification ISO 27001,
- renforcer les règles relatives aux accès à l'information,
- promouvoir la culture de sécurité et capitaliser les connaissances en matière de sécurité de l'information,
- suivre mensuellement des indicateurs de performance associés.

L'application opérationnelle de cette politique de sécurité n'est possible que par l'engagement des collaborateurs à contribuer et à promouvoir la sécurité au sein de leurs activités quotidiennes.
Les managers font preuve de leadership pour faire appliquer les règles de sécurité qui seront définies par le RSSI.
J'ai délégué la mise en œuvre de notre politique sécurité à Mme Laura Najberg en tant que responsable conformité. Cependant, je veille personnellement à l'efficacité des dispositions qui sont prises et à leur amélioration.

Le : 18 avril 2021
Marc TAIEB
Le président