

## La Politique de Sécurité des Systèmes d'Information du Groupe CIS contribue à :

- Assurer la continuité des activités du Groupe CIS.
- Prévenir la fuite d'Informations sensibles.
- Renforcer la confiance des collaborateurs du Groupe dans l'utilisation des moyens mis à leur disposition.

## Cette politique définit les mesures de sécurité applicables aux Systèmes d'Information du Groupe CIS. Il s'appuie sur 10 principes stratégiques :

1. Lorsque la maîtrise de ses Systèmes d'Information l'exige, le Groupe CIS fait appel à des opérateurs et des prestataires de confiance.
2. Tout système d'information du Groupe CIS doit faire l'objet d'une analyse de risques permettant une prise en compte préventive de sa sécurité, adaptée aux enjeux du système considéré. Cette analyse s'inscrit dans une démarche d'amélioration continue de la sécurité du système, pendant toute sa durée de vie. Cette démarche doit également permettre de maintenir à jour une cartographie précise des systèmes d'information en service.
3. Les moyens humains et financiers consacrés à la sécurité des Systèmes d'Information du Groupe CIS doivent être planifiés, quantifiés et identifiés au sein des ressources globales des Systèmes d'Information.
4. Des moyens d'authentification forte des collaborateurs du Groupe CIS sur les Systèmes d'Information doivent être mis en place.
5. Les opérations de gestion et d'administration des Systèmes d'Information du Groupe CIS doivent être tracées et contrôlées.
6. La protection des Systèmes d'Information doit être assurée par l'application rigoureuse de règles précises. Ces règles font l'objet des lignes d'orientation de la sécurité des systèmes d'information.
7. Chaque collaborateur du Groupe CIS, en tant qu'utilisateur d'un Système d'Information, doit être informé de ses droits et devoirs mais également formé et sensibilisé à la cybersécurité. Les mesures techniques mises en place par le Groupe CIS dans ce domaine doivent être connues de tous.
8. Les administrateurs des Systèmes d'Information doivent appliquer, après formation, les règles élémentaires d'hygiène informatique.
9. Les produits et services acquis par les différents départements et destinés à assurer la sécurité des Systèmes d'Information du Groupe CIS doivent faire l'objet d'une évaluation et d'une validation préalable de leur niveau de sécurité par le responsable de la Sécurité des Systèmes d'Information du Groupe CIS.
10. Les informations considérées comme sensibles, en raison de leurs besoins en confidentialité, intégrité ou disponibilité, sont hébergées sur le Système d'Information du Groupe CIS.

Régis Arnoux, *Chairman & CEO*