



POLITIQUE DE SÉCURITÉ DE L'INFORMATION

Table des matières

1.INTRODUCTION	4
2.PORTEE	4
3.OBJECTIFS DE SECURITE DE L'INFORMATION	4
4.PRINCIPES DE SECURITE DE L'INFORMATION	5
5.RESPONSABILITÉS	6
6.CONTROLE ET AUDIT	7
7.REVISION DE LA POLITIQUE	7

INFORMATIONS IMPORTANTES SUR CE DOCUMENT	
Identification du document	Politique de sécurité de l'information
Version	1.0
Responsable principal de son contrôle	Responsable de la sécurité
Auteur	CIO
Organe d'approbation	Comité de direction
Date d'approbation	15 décembre 2021

1. Introduction

Le comité de direction a adopté, lors de sa session du 15 décembre 2021, la présente Politique de sécurité de l'information, qui détermine les principes et des lignes directrices selon lesquels ATLS (ci-après la « Société ») protégera ses informations conformément à la réglementation applicable, à ses valeurs éthiques et à toute autre réglementation interne applicable.

La présente Politique sera disponible sur l'intranet pour tous les employés et sur le site internet de l'entreprise pour toutes les parties prenantes de la Société. La Politique fera également l'objet d'actions de communication, de formation et de sensibilisation appropriées pour sa compréhension et sa mise en œuvre opportunes.

2. Portée

La présente Politique s'applique à ATLS et lie tous ses employés, indépendamment de la position et du poste qu'ils occupent.

ATLS garantira la protection des informations, indépendamment de la manière dont celles-ci sont communiquées, partagées ou stockées. Cette protection s'applique à la fois aux informations présentes au sein de la Société et aux informations partagées avec des tiers.

La Sécurité de l'information correspond à la conservation et à la protection :

- Des informations détenues par la Société, qu'elles soient stockées sur des systèmes propres ou des systèmes tiers.
- Des informations détenues par des tiers stockées sur des systèmes de la Société.

Conformément à la Politique, ATLS pourra établir des procédures et des instructions pour permettre la mise en œuvre et le respect des obligations contractées, ainsi que pour l'adapter aux différentes législations locales applicables au groupe.

La mise en œuvre de cette Politique vient également compléter d'autres règles internes contraignantes, telles que la politique de conformité en matière de protection des données à caractère personnel et de confidentialité, et celles qui réglementent les questions liées à l'information de la Société.

3. Objectifs de sécurité de l'information

La présente Politique établit le cadre de référence par lequel ATLS définit les principes et les règles de base relatifs à la protection de l'information gérée par la Société et dont les objectifs sont les suivants :

- Comprendre et gérer les **risques** opérationnels et stratégiques en matière de sécurité de l'information afin qu'ils restent à des niveaux acceptables pour la Société.
- Garantir le degré de **confidentialité** nécessaire à chaque type d'information et prévenir la fuite d'information.
- Maintenir l'**intégrité** de l'information, en évitant toute altération par rapport au moment où elle a été générée par les propriétaires ou les responsables de celle-ci.
- Garantir la **disponibilité** de l'information, sur tous les supports et chaque fois que nécessaire, en assurant la continuité de l'activité et le respect des obligations auxquelles la Société est tenue.

4. Principes de sécurité de l'information

La présente Politique s'inscrit dans le cadre des recommandations relatives aux meilleures pratiques liées à la sécurité de l'information, et est conforme à la législation en vigueur en matière de protection des données à caractère personnel et aux réglementations qui, dans le domaine de la sécurité de l'information, peuvent affecter la Société.

De plus, ATLS définit les principes de base suivants qui constituent des lignes directrices fondamentales quant à la sécurité de l'information et qui doivent toujours être appliqués lors de toute activité liée au traitement de l'information :

- **Utilisation des systèmes d'information.** L'utilisation des systèmes d'information est limitée exclusivement à la réalisation de tâches en lien avec le poste de travail. Ces moyens et systèmes ne sont pas destinés à l'usage personnel et ne peuvent être utilisés à aucune fin illicite.
- **Sécurité de l'information dans les systèmes développés.** Les environnements de développement et de production seront maintenus dans des systèmes indépendants. Le développement et la maintenance des systèmes d'information doivent envisager la mise en œuvre des spécifications de sécurité.
- **Séparation des tâches.** Les risques liés à l'absence de séparation des tâches et à la réalisation individuelle des fonctions critiques pour l'entreprise doivent être évités.
- **Rétention d'information.** Des périodes de rétention de l'information par catégories seront établies, lorsque cela est nécessaire aux besoins opérationnels ou de conformité réglementaires.
- **Ressources nécessaires.** Un financement sera réservé à la gestion opérationnelle des contrôles liés à la sécurité de l'information et des processus de gestion pour sa mise en œuvre et sa maintenance.
- **Risques.** La Société assume la prise de risques et tolère ceux qui, sur la base des informations disponibles, sont compréhensibles, contrôlés et gérés lorsque cela est nécessaire.
- **Continuité.** Un processus de gestion de la continuité sera mis en place afin de garantir la récupération des informations critiques pour la Société en cas de catastrophe, en minimisant le temps d'indisponibilité à des niveaux acceptables.
- **Conformité.** Les systèmes d'information et de communication de la Société devront être constamment conformes aux exigences de la législation en vigueur, ainsi qu'à la réglementation interne de développement applicable.
- **Exécution légale.** Les situations susceptibles d'exposer l'organisation à la violation des lois et des normes juridiques ne seront pas tolérées.

5. Responsabilités

La responsabilité de la protection de l'information et des systèmes qui la traitent, stockent ou transmettent s'étend à tous les niveaux organisationnels et fonctionnels d'ATLS, chacun dans la mesure où il est concerné, tel que décrit ci-après :

- Tous les employés de la Société doivent connaître et respecter la Politique et sont tenus de garantir la confidentialité de l'information utilisée dans leur environnement professionnel et de communiquer, de toute urgence, les incidents ou problèmes de sécurité éventuels détectés.
- L'utilisation des systèmes ou services numériques par les employés, y compris en particulier le courrier électronique et les services de messagerie instantanée, est limitée à des fins licites et exclusivement liées aux tâches du poste de travail. Par conséquent, ces moyens et systèmes ne sont pas destinés à l'usage personnel et ne peuvent être utilisés à aucune fin illicite.
- Les contrats avec des tiers qui impliquent l'accès de ces derniers aux informations, notamment les contrats de prestation de services ou les contrats de sous-traitance, doivent veiller à ce que les fournisseurs, le personnel sous-traité et toute entreprise externe qui utilisent ou consultent les informations, connaissent et respectent la Politique dans la mesure où ils sont concernés, et sont tenus au secret professionnel et à la confidentialité des informations utilisées dans leurs relations avec la Société.
- Le responsable de la sécurité de l'information est chargé de mettre en œuvre la présente Politique et de veiller à ce qu'elle soit respectée, ainsi que toutes les exigences découlant des lois, des normes et des bonnes pratiques applicables en matière de sécurité de l'information. Par conséquent, il est chargé de :
 - Mettre en œuvre une stratégie de sécurité de l'information qui garantisse le respect des principes de base de la présente Politique.
 - Établir et réviser les contrôles pertinents pour garantir le respect de la présente Politique et de ses règles de d'application.
 - Prévenir, détecter et réagir à tout incident en matière de sécurité de l'information et agir conformément au Plan d'intervention en cas d'incident.
 - Promouvoir des activités de formation et de sensibilisation en matière de processus de sécurité de l'information.
 - Définir une approche d'amélioration continue.
 - Veiller au respect de la législation en vigueur dans le domaine des compétences qui lui sont conférées par la présente Politique.
 - Réviser, actualiser et communiquer tout changement résultant de modifications de la présente Politique.

6. Contrôle et audit

ATLS se réserve expressément le droit d'adopter, conformément au principe de proportionnalité, les mesures de surveillance et de contrôle nécessaires pour s'assurer de l'utilisation correcte des systèmes mis à la disposition de ses employés, notamment le contenu des communications et des dispositifs, en respectant la législation en vigueur et la dignité du salarié. La communication et l'acceptation de la présente Politique produiront les effets de notification préalable au travailleur.

La Société sera soumise à des révisions et à des contrôles réguliers, ainsi qu'à des audits internes et externes pour évaluer la conformité globale de la présente Politique.

7. Révision de la Politique

L'adoption de la présente Politique implique que sa mise en œuvre bénéficie du soutien du comité de direction afin qu'elle atteigne tous les objectifs qui y sont établis, ainsi que pour satisfaire à toutes ses exigences.

La présente Politique de sécurité de l'information sera revue et mise à jour le cas échéant, afin de l'adapter aux changements éventuels, qu'ils soient de type opérationnel, juridique, réglementaire ou contractuel, afin de garantir son adéquation permanente à la réalité de la Société.