Politique de Sécurité de l'Information

MOTIVATION

Le manque de contrôle des entreprises sur la manière dont les données et les informations sont générées, sur le lieu où elles sont stockées et sur les destinataires auxquels elles sont transmises, comporte un risque d'incidents de sécurité et de conformité réglementaire susceptibles d'avoir un impact négatif sur l'activité elle-même. La sécurité de l'information constitue en effet un actif primordial de l'entreprise, et la mise en œuvre de mesures efficaces peut représenter une stratégie qui, avec le temps, se transforme en avantage concurrentiel.

Pour cette raison, Artificialy SA, spécialisée dans les solutions d'intelligence artificielle, a toujours été à l'avant-garde de la protection et de la sécurité de l'information. Une mesure fondamentale à cet égard a été la mise en place d'un Système de Management de la Sécurité de l'Information, un ensemble de processus organisationnels, techniques et procéduraux fondés sur les meilleures pratiques et les normes de référence, également conforme aux directives et à la norme internationale ISO/IEC 27001:2022.

OBJECTIFS

L'objectif du Système de Management de la Sécurité de l'Information d'Artificialy SA est de garantir un niveau de protection et de sécurité adapté à la circulation des informations au sein de l'organisation, afin de mener à bien la conception, le développement et la fourniture des services de l'entreprise.

Sans procédures d'identification, d'évaluation et d'analyse des risques, les menaces de sécurité auxquelles les services et procédures de l'entreprise sont exposés quotidiennement pourraient compromettre leur bon fonctionnement, avec des conséquences économiques possibles.

L'ensemble des mesures organisationnelles, techniques et procédurales établies par le Système de Management de la Sécurité de l'Information d'Artificialy SA répond aux exigences de sécurité fondamentales suivantes :

- **Confidentialité** : l'accès aux informations n'est autorisé qu'aux personnes disposant des privilèges appropriés.
- **Intégrité** : la gestion des informations (y compris leur modification) est soumise à des contraintes précises établies par la gouvernance de l'entreprise.
- **Disponibilité** : les utilisateurs autorisés peuvent accéder librement aux informations chaque fois qu'ils en ont besoin dans le cadre des processus opérationnels, et la récupération se fait de manière rapide et intuitive.

Artificialy SA entend se positionner dans le domaine de la sécurité de l'information comme :

- Un fournisseur fiable et compétent dans la préservation de l'image de l'entreprise.
- Un pôle où les actifs informationnels de l'entreprise sont stockés, préservés et protégés.
- Un facilitateur de la continuité des activités pour les processus opérationnels.
- Un outil pleinement conforme à la réglementation applicable et obligatoire, ce qui se traduit par le développement de l'expertise de l'entreprise en matière de sécurité de l'information.

CONTENU DE LA POLITIQUE

Toute information nécessaire à la réalisation des activités internes, des données de produit/service à leur configuration, doit être protégée pendant tout son cycle de vie, de la création à l'utilisation, jusqu'à son élimination. Le Système de Management de la Sécurité de l'Information fait partie de ce processus, permettant une gestion de l'information sûre, précise et fiable, ainsi qu'une récupération rapide des informations.

Conformément à la norme ISO/IEC 27001:2022 en vigueur, parmi les mesures préventives requises par le Système de Management de la Sécurité de l'Information figure l'évaluation obligatoire des risques de sécurité et de leur impact potentiel sur l'entreprise, qui doit être effectuée périodiquement par le Responsable de la Sécurité de l'Information. Le Responsable de la Sécurité de l'Information doit vérifier si les exigences de sécurité mentionnées ci-dessus sont respectées, analyser les facteurs critiques ayant conduit à des incidents de sécurité et les replacer dans le contexte plus large des changements stratégiques, commerciaux et technologiques déjà mis en œuvre ou à mettre en œuvre.

L'objectif de cette analyse est d'évaluer le risque associé à chaque actif à protéger face aux menaces identifiées. La procédure adoptée par le Responsable de la Sécurité de l'Information pour effectuer cette évaluation est partagée avec la Direction, qui doit approuver le document décrivant la méthodologie à appliquer. En outre, la Direction contribue également à définir les paramètres utilisés pour déterminer le niveau de risque. Une fois l'évaluation réalisée par le Responsable de la Sécurité de l'Information, les résultats sont examinés conjointement avec la Direction, qui détermine si le niveau de risque est acceptable selon les indicateurs préalablement établis. Enfin, lorsque cela est jugé nécessaire, des mesures d'atténuation des risques et des actions visant à améliorer la sécurité du système sont définies en fonction des priorités, du budget de l'entreprise et de la nécessité de se conformer à la réglementation applicable. Toutes les décisions sont prises en tenant compte de la valeur des informations à protéger et

de la survenue d'événements susceptibles d'affecter significativement la sécurité du système.

RESPONSABILITÉS

Les responsabilités sont réparties comme suit :

LE PERSONNEL, qui est responsable du respect de la politique de sécurité de l'information convenue et doit signaler au responsable compétent toute anomalie constatée.

LE COMITÉ DE SÉCURITÉ DE L'INFORMATION, qui se réunit au moins tous les six mois. Il est composé de la Direction et du Responsable de la Sécurité de l'Information, bien que des employés disposant des compétences techniques nécessaires puissent également être associés à l'évaluation de questions spécifiques. La Direction est responsable de la définition des priorités et de la promotion des initiatives en matière de sécurité de l'information, tout en veillant à leur alignement avec les stratégies de l'entreprise et le budget alloué au projet.

LE RESPONSABLE DE LA SÉCURITÉ DE L'INFORMATION, qui est chargé de la rédaction et de la conception du Système de Management de la Sécurité de l'Information. Plus précisément, le Responsable de la Sécurité de l'Information effectue l'analyse et la gestion des risques en identifiant les critères et méthodologies les plus appropriés, et est responsable de la tenue de la documentation nécessaire, y compris les procédures de classification des documents. Ce rôle comprend également la proposition de mesures de sécurité adéquates et l'examen des incidents de sécurité, ainsi que des actions correctives associées. En outre, le Responsable de la Sécurité de l'Information s'engage à promouvoir une culture de la sécurité de l'information et à proposer des programmes de formation pour le personnel.

LES PARTIES EXTERNES qui interagissent avec Artificialy SA doivent respecter les principes de sécurité spécifiés et, lorsque cela n'est pas explicitement stipulé dans le contrat, signer un accord de confidentialité pour la mission qui leur est confiée.

APPLICABILITÉ

La présente Politique de Sécurité de l'Information s'applique à l'ensemble des organes internes et externes de l'entreprise et est contraignante pour tout le personnel d'Artificialy SA. Elle s'applique également à toute partie externe ayant connaissance d'informations gérées par l'entreprise. Cela nécessite une réglementation préalable des accords, afin de garantir que la communication avec les parties externes se déroule dans le respect des règles et réglementations applicables.

RÉVISION

Artificialy SA veille à la vérification périodique de l'efficacité et de l'efficience du Système de Management de la Sécurité de l'Information. Lorsque cela est nécessaire, et conformément au contexte et aux objectifs de l'entreprise, elle adopte les mesures requises pour améliorer les politiques de sécurité et garantir leur bonne mise en œuvre, afin d'assurer l'exécution continue et sécurisée de tous les processus de l'entreprise.