deepcloud

POLITIQUE DE SÉCURITÉ DE L'INFORMATION

ISMS MANAGER
DEEPCLOUD AG
Wittenbach

ID : DC021 - FR
Version : 1.1
Date : 8.9.2021

CONTROLE DES DOCUMENTS

Modifications du procès-verbal

Date	Version	Statut (ébauche/révision)	Auteur	Description
27.8.2021	1.0	Finale	CE1 / ISMS Manager	Première version
8.9.2021	1.1	Approuvé	ISMS Manager	Mise à jour de l'introduction et modifications sémantiques mineures (sans rapport avec le contenu)

Révision et approbation/validation

Date	Version	Révision/approbation	Autorisé à modifier et à approuver	Remarques
8.9.2021	1.1	Approbation	CEO	

REFERENCES A DES DOCUMENTS EXTERNES

Date	Version	ID doc	Nom et description	Nom du document/lien

REFERENCES A DES DOCUMENTS INTERNES

Date	Version	ID doc	Nom et description	Nom du document/lien

LISTE DE DIFFUSION

Date	Nom	Nom du document/lien
20.9.2021	Public	-

1. SOMMAIRE

2. Introduction

DeepCloud AG (ci-après "Entreprise") accorde une importance primordiale à la protection des données et de la structure organisationnelle (technologique et physique) pour garantir la sécurité de l'information. Le *système de management de la sécurité de l'information* (ci-après "ISMS") mis en œuvre au sein de l'entreprise est conçu pour être toujours actuel et garantir le respect des mesures de sécurité énumérées ci-après :

1. **Confidentialité**, toutes les informations/données ne sont accessibles qu'aux personnes et/ou processus dûment autorisés.
2. **Intégrité**, la cohérence des bases de données et des informations stockées est protégée contre toute modification non autorisée.
3. **Disponibilité**, les utilisateurs autorisés peuvent accéder aux informations/données dont ils ont besoin lorsqu'ils en font la demande.
4. **Contrôle**, les données sont gérées par des processus et des outils contrôlés et sécurisés.
5. **Authenticité**, une source d'information fiable est garantie.
6. **Protection des données**, la protection et le contrôle des données personnelles sont garantis.

Les produits et services offerts par l'entreprise par le biais de son infrastructure technologique sont garantis par les niveaux de sécurité définis dans l'ISMS; à savoir :

- Fiabilité du système pour la gestion des processus et de l'information
- Obligation de diligence maximale pour l'image de l'entreprise
- Respect absolu du Service Level Agreement convenu avec les clients
- Satisfaction des clients
- Conformité aux directives en vigueur et à la norme internationale de sécurité

L'ISMS mis en œuvre dans l'entreprise répond aux exigences de la norme ISO/CEI 27001:2013 et à la législation relative à la sécurité de l'information dans le cadre des activités de l'entreprise.

3. Champ d'application

Cette présente politique de sécurité de l'information s'applique à l'ensemble du personnel interne et aux tiers impliqués dans la gestion de l'information, ainsi qu'à tous les processus et ressources engagés dans la conception, la mise en œuvre, la mise en service et la fourniture continue des services de l'entreprise.

4. Principes

Le terme "sécurité" est défini de manière très large dans l'entreprise et concerne la perte de biens matériels et immatériels tels que les informations ainsi que les risques pouvant porter atteinte à la poursuite de ses activités. L'ISMS mis en place a été développé pour identifier et prévenir ces risques rapidement.

La valeur ajoutée de la politique d'information et de sécurité mise en place par l'entreprise réside dans sa capacité à réagir avant qu'un événement dommageable ne se produise. Cela est possible dans la mesure où chaque membre de l'organisation agit avec objectivité et met à profit son expérience pour atteindre un niveau élevé d'efficacité et d'efficience dans la gestion de la sécurité des informations.

La politique de sécurité de l'information de l'entreprise est fondée sur les principes suivants :

- Garantir une parfaite connaissance des informations et une évaluation de leur degré critique afin de faciliter la mise en place d'un niveau de protection approprié.
- Garantir un accès légal et sécurisé aux informations afin d'empêcher tout traitement non autorisé.
- Veiller à ce que l'organisation et les tiers collaborent au traitement des informations en introduisant des procédures visant à maintenir un niveau de sécurité approprié.
- Veiller à ce que l'organisation et les tiers impliqués dans le traitement des informations soient pleinement conscients des problèmes de sécurité.
- Veiller à ce que les anomalies et les incidents affectant le système d'information et la sécurité de l'entreprise soient immédiatement identifiés, documentés et correctement gérés par des systèmes efficaces de prévention, de communication et de réponse afin de minimiser l'impact sur l'activité.
- Veiller à ce que l'accès aux bureaux et aux différents bâtiments de l'entreprise soit réservé au personnel autorisé afin de garantir la sécurité des lieux et des biens.
- Garantir le respect des dispositions légales et des obligations de sécurité définies dans les contrats avec les tiers.
- Garantir la détection de comportements anormaux, d'événements et de failles des systèmes d'information afin d'accroître la sécurité et la disponibilité des services et des informations.
- Garantir la continuité et la reprise des activités en cas d'incident grave par l'application de procédures de sécurité établies.

La politique de sécurité de l'information est inscrite dans l'ISMS. Elle est actualisée en permanence afin de garantir une constante amélioration et est communiquée à l'organisation, aux tiers et aux clients par les canaux de communication appropriés.

5. Objectifs

Conformément aux principes susmentionnés, l'entreprise définit les objectifs suivants, qui doivent être pris en compte dans tous les processus de travail :

- Gérer la sécurité de l'information, définir des objectifs appropriés, mettre à disposition des ressources adéquates, préparer des politiques et des procédures de sécurité spécifiques à mettre en œuvre dans chaque département, en veillant toujours à respecter pleinement les dispositions légales et réglementaires.
- Communiquer des stratégies, des objectifs et des buts en matière de sécurité de l'information afin qu'il y ait un réel échange et un accord sur les comportements et les mesures à prendre.
- Minimiser les risques et éviter les failles de sécurité afin de protéger les personnes, les biens et l'entreprise contre toute menace, et garantir les normes, les objectifs, la compétitivité, la marque et l'image de l'entreprise.
- Impliquer l'ensemble des collaborateurs et des fournisseurs par le biais de communications et de formations visant à accroître les connaissances, les compétences et la sensibilisation aux aspects de la sécurité de l'information, tant dans la gestion des activités quotidiennes que dans celle des incidents susceptibles de compromettre la poursuite des activités de l'entreprise.

- Garantir un retour rapide à la normale en cas d'urgence et de crise, limiter les dommages et les pertes, protéger les personnes et les biens de l'entreprise.
- Surveiller les processus internes afin de vérifier en permanence l'adéquation du système et d'identifier les mesures d'amélioration possibles.
- Améliorer l'ISMS pour l'adapter à l'évolution des exigences globales, commerciales et légales.

Les principes susmentionnés et les objectifs définis font partie intégrante du travail quotidien de l'entreprise. Pour atteindre ces objectifs, toutes les mesures techniques, organisationnelles et opérationnelles nécessaires seront prises et contrôlées dans le cadre d'un processus continu.

6. RESPONSABILITE DE LA POLITIQUE DE SECURITE DE L'INFORMATION

La direction est chargée de maintenir l'ISMS à jour et de l'adapter à l'évolution de l'environnement des affaires et du marché en évaluant toutes les mesures sur la base des éléments suivants :

- Développements importants des affaires
- Analyse des risques liés aux nouvelles menaces
- Incidents de sécurité pertinents
- Modifications du contexte réglementaire ou juridique relatif au traitement sécurisé des informations

La responsabilité de la protection des personnes et des ressources de l'entreprise incombe à l'organisation. Toutes les personnes qui gèrent, exploitent et contrôlent les processus de l'entreprise doivent garantir un niveau de protection approprié en utilisant les outils et les ressources fournis par l'entreprise.

Les responsables des différentes fonctions et départements doivent s'assurer que cette politique de sécurité de l'information est comprise et mise en œuvre en conséquence par tous les collaborateurs et fournisseurs concernés.