Politique de sécurité de l'information

1 Objet

SOIK Corporation (ci-après dénommée "l'Entreprise") utilise de nombreux actifs informationnels dans le cadre de son activité de consulting et de santé numérique et de la gestion de ses employés (ci-après dénommée "l'Activité"), et par conséquent, l'Entreprise reconnaît que la réalisation correcte de la sécurité de l'information et la protection des actifs informationnels sont des exigences essentielles pour promouvoir des activités d'entreprise basées sur la confiance de la société et qu'il s'agit d'une responsabilité sociale sérieuse. Par conséquent, compte tenu de l'importance de la sécurité de l'information, la société a établi la présente politique de sécurité de l'information (ci-après dénommée "la politique") et établira, mettra en œuvre, maintiendra et améliorera un système de gestion de la sécurité de l'information afin de mettre spécifiquement en œuvre la politique.

2 Définition de la sécurité de l'information

La sécurité de l'information est définie comme le maintien de la confidentialité, de l'intégrité et de la disponibilité.

(1) Confidentialité.

Il s'agit de protéger les actifs informationnels contre tout accès non autorisé et toute fuite vers des personnes non autorisées à s'y référer.

(Caractéristique consistant à ne pas permettre l'utilisation ou la divulgation d'informations à des personnes, entités ou processus non autorisés).

(2) Intégrité.

Signifie que les actifs informationnels sont protégés contre la falsification ou l'erreur et sont maintenus exacts et complets.

(Caractéristique d'exactitude et d'exhaustivité).

(3) Disponibilité.

Signifie que les actifs informationnels sont protégés contre les pertes, les dommages ou les pannes de système et qu'ils sont disponibles lorsque cela est nécessaire.

(Caractéristiques d'accès et de disponibilité pour une utilisation à la demande des entités autorisées)

3 Champ d'application

Cette politique s'applique à tous les actifs informationnels gérés par l'Entreprise. Le champ d'application des actifs informationnels ne se limite pas aux dispositifs électroniques et aux données électroniques, mais inclut toutes les formes d'actifs informationnels, y compris le papier.

(1) Organisation

SOIK Corporation (tous les employés)

(2) Installations

Siège social (Adresse : 1861 Uza, Yomitan Village, Nakagamigun, Okinawa 904-0328, Japon)

(3) Activités

Santé numérique et activité de conseil, administration générale

(4) Actifs

Documents, données, systèmes d'information et réseaux liés aux opérations et aux divers services susmentionnés.

4 Mise en œuvre

Conformément à la présente politique et au système de gestion de la sécurité de l'information de la société, les points suivants doivent être mis en œuvre

(1) Objectifs de sécurité de l'information

Des objectifs de sécurité de l'information conformes à la présente politique et tenant compte des exigences applicables en matière de sécurité de l'information, des résultats des évaluations des risques et des réponses aux risques doivent être établis et communiqués à tous les employés, et doivent être revus de temps à autre en réponse aux changements de notre environnement, et périodiquement même en l'absence de changements.

(2) Traitement des actifs informationnels

a) Les droits d'accès ne sont accordés qu'à ceux qui en ont besoin pour leur travail.

b) La gestion est effectuée conformément aux exigences légales et réglementaires, aux exigences contractuelles et aux dispositions du système de gestion de la sécurité de l'information de l'entreprise.

c) Les actifs informationnels sont classés et gérés de manière appropriée en fonction de leur importance en termes de valeur, de confidentialité, d'intégrité et de disponibilité.

d) Un contrôle continu est effectué pour s'assurer que les actifs informationnels sont correctement gérés.

(3) Évaluation des risques

a) Des évaluations des risques sont effectuées, et des réponses appropriées aux risques sont mises en œuvre et des mesures de contrôle introduites pour les actifs informationnels jugés les plus importants en termes de caractéristiques de l'entreprise.

b) Les causes des incidents liés à la sécurité de l'information sont analysées et des mesures sont prises pour éviter qu'ils ne se reproduisent.

(4) Gestion de la continuité des activités

L'interruption des activités due à des catastrophes ou à des pannes est réduite au minimum et la capacité de continuité des activités est assurée.

(5) Formation

L'éducation et la formation en matière de sécurité de l'information sont dispensées à tous les employés.

(6) Respect des règlements et des procédures

Les règlements et les procédures du système de gestion de la sécurité de l'information sont respectés.

(7) Conformité aux exigences légales, réglementaires et contractuelles

Les exigences légales et réglementaires ainsi que les exigences contractuelles relatives à la sécurité de l'information sont respectées.

(8) Amélioration continue

L'amélioration continue du système de gestion de la sécurité de l'information est prise en compte.

5 Responsabilités, obligations et sanctions

La responsabilité du système de gestion de la sécurité de l'information, y compris la présente politique, incombe au directeur représentatif, qui est tenu de veiller à ce que tous les employés dans le champ d'application se conforment aux règles et procédures établies. Les employés qui ne respectent pas leurs obligations et qui commettent des infractions sont sanctionnés comme le prévoit le règlement du travail. Les employés des sous-traitants sont traités conformément aux contrats définis individuellement.

6 Révision périodique

Le système de gestion de la sécurité de l'information est revu, entretenu et géré de manière régulière et selon les besoins.

Etabli : 01.09.2022.

Dernière révision : 01.09.2022

Représentant Directeur : Kuniyuki Furuta