POLITIQUE DE LA SECURITE et de la CONFIDENTIALITE DE L'INFORMATION DE NOTRE GROUPE 2018

1. Sommaire de la politique de Sécurité

- La politique de Sécurité de l'information a pour objet d'assurer un niveau adéquat de sécurité en termes de confidentialité, disponibilité et d'intégrité des actifs informationnels de GROSPIRON INTERNATIONAL et CSU contre toutes les menaces dont elles pourraient être l'objet.
- La politique de la Sécurité de l'information est déterminée selon les enjeux internes et externes et considère l'influence sur sa capacité à gérer les risques et atteindre les objectifs.
- Le système de management de la Sécurité de l'Information a pour fonction d'établir, mettre en œuvre, surveiller, tenir à jour et améliorer en continu des processus et mesures reliés à la sécurité de l'information basé sur une approche du risque lié à l'activité.
- La politique sur la protection des données intègre le droit d'accès, de rectification, d'opposition, de portabilité et d'effacement des données pour les prospects, clients ou salariés.

2. Introduction

- L'information et les processus, systèmes et réseaux qui en permettent le traitement constituent des biens importants pour GROSPIRON INTERNATIONAL ET CSU dans la réalisation de leur mission d'affaires.
- GROSPIRON INTERNATIONAL et CSU se doivent de s'assurer du respect de l'intégrité, de la confidentialité et de la disponibilité de toute information produite ou conservée au sein du domaine d'application du SMSI.
- GROSPIRON INTERNATIONAL et CSU doivent s'assurer de la protection de leur actifs informationnels contre toute menace interne ou externe, accidentelle ou délibérée.

3. Domaine d'application du SMSI

- Cette politique soutient la politique de sécurité et la politique de sécurité de l'information.
- Cette politique tient compte du contexte externe et interne et des exigences des parties prenantes.
- Cette politique tient compte du règlement général de la protection des données (RGPD).
- Cette politique s'applique aux activités :
  - Gestion administrative du déménagement à l'international et au national
  - Services de relocations

4. Objectifs du SMSI

- Atteindre les objectifs et améliorer la sécurité en interne et également des parties prenantes.
- Assurer la continuité des activités métier critiques.
- Assurer que toute information traitée, conservée, échangée ou publiée par GROSPIRON INTERNATIONAL et CSU soit d'une absolue intégrité.
- Garantir que toutes les informations importantes pour GROSPIRON INTERNATIONAL et CSU seront contrôlées et stockées selon des procédures de maintien de la confidentialité appropriées.
- Assurer le choix de mesures de sécurité adéquates et proportionnées qui protège les actifs et donnent confiance aux parties intéressées.
- Assurer une gestion efficace et efficiente du management de la sécurité de l'information.
- Assurer la mise en place et l'application de la protection du traitement des données des parties prenantes.

5. Principes de la politique SMSI

- GROSPIRON INTERNATIONAL et CSU doivent établir, mettre en œuvre, exploiter, surveiller, tenir à jour et améliorer un SMSI documenté basé sur une approche du risque lié à l'activité et en conformité avec l'ensemble des exigences de la norme ISO 27001.
- GROSPIRON INTERNATIONAL et CSU doivent tenir compte de toutes les exigences légales (Exemple RGDP) réglementaires et contractuelles en vigueur dans le management du SMSI afin d'éviter toute violation de leurs obligations légales, statutaires, réglementaires ou contractuelles et des exigences de sécurité.
- Les exigences légales et réglementaires seront respectées en priorité, même si elles sont contradictoires avec la politique ici décrite.
- GROSPIRON INTERNATIONAL et CSU doivent établir et mettre en œuvre un programme de management du risque documenté conforme aux exigences de la norme ISO 27001. Des critères d'évaluation et d'acceptation du risque doivent être établis, formalisés et approuvés par la direction.
- Cette politique a été approuvée par la direction et est l'objet d'un réexamen annuel.

6. Responsabilités

- La direction doit diriger, soutenir, promouvoir et communiquer la politique SI en place.
- La direction a la responsabilité d'assurer que des objectifs et des plans pour le SMSI soient établis et revue annuellement lors de la revue de direction, que les rôles et responsabilités pour la sécurité de l'information soient définit, qu'un programme à la sensibilisation de la sécurité soit communiqué, qu'un audit interne soit mené au moins une fois par année et de fournir les ressources nécessaires au maintien et à l'amélioration du SMSI.

- La direction doit diriger, soutenir, promouvoir et communiquer la politique SI en place.

Le garant de la protection des données et/ou le responsable de la sécurité de l'information est habilité à intervenir sur tous les aspects de la sécurité de l'information et s'assure de la conformité et de l'efficacité du SMSI. Par des directives administratives, préalablement soumises à la direction générale, il décide, en général, de tout ce qui est nécessaire au fonctionnement efficace du SMSI.

- Chaque directeur a la responsabilité d'assurer, que les personnes qui travaillent sous son contrôle protègent l'information conformément aux politiques de GROSPIRON INTERNATIONAL et CSU.
- Les intervenants de GROSPIRON INTERNATIONAL et CSU (direction, salariés, contractants et utilisateurs tiers) doivent être sensibilisés aux risques pesant sur la sécurité de l'information, de leurs responsabilités, et de la nécessité de respecter les politiques pour assurer une protection adéquate de l'information dans le cadre de leur activité normale.

7. Résultats attendus

- Des mesures de sécurité de l'information adéquates et proportionnées seront en œuvre afin d'assurer la protection des actifs et donner confiance aux parties intéressées.
- Les décisions en matière de sécurité de l'information seront basées sur l'évaluation du risque auquel sont confrontées GROSPIRON INTERNATIONAL et CSU.
- Les exigences légales, réglementaires et contractuelles de GROSPIRON INTERNATIONAL et CSU en matière de sécurité de l'information seront respectées.
- Les notions de « conception de la vie privée » et « l'évaluation d'impact sur la vie privée » des données seront intégrées dans le Groupe.

8. Politiques connexes

- La politique de gestion des ressources humaines.
- La politique sur la formation et le développement des compétences du personnel.

Le 16 mai 2018

Président
Jean Luc Haddad