Sécurité de l'information

Historique

Toutes	Création	01/01/2016
Page	**Changement**	**Date**

Auteur / fonction	Vérifié / fonction	Approuvé / fonction
/	/	/

1. Objet

La politique de sécurité de l'information a pour objet la stratégie, l'organisation et les responsabilités en matière de protection de la sécurité de l'information contre toute menace interne, externe, délibérée ou accidentelle.

2. Finalité

La politique de sécurité de l'information a pour finalité d'assurer la continuité de l'activité de l'organisation en réduisant les risques et les impacts d'incidents de sécurité de l'information.

3. Domaine d'application

La politique de sécurité de l'information s'applique à l'ensemble du personnel, à tous les départements et actifs numériques et papier de notre organisation.

4. Responsabilité

Le responsable sécurité de l'information (RSI) a l'autorité de l'écriture et de la mise à jour de la politique de sécurité de l'information. Il est garant de son application et de sa communication. La politique de sécurité de l'information est validée par le directeur.

5 Documents

Descriptions de fonction

6. Exigences de la norme ISO 27001 : 2013

5.2 Politique
La direction doit établir une politique de sécurité de l'information qui :
a) est adaptée à la mission de l'organisation;
b) inclut des objectifs de sécurité de l'information (voir 6.2) ou fournit un cadre pour l'établissement de ces objectifs; c)
l'établissement de ces objectifs ;
c) inclut l'engagement de satisfaire aux exigences applicables en matière de sécurité de l'information; et
d) inclut l'engagement d'œuvrer pour l'amélioration continue du système de management de la sécurité de l'information.
La politique de sécurité de l'information doit :
e) être disponible sous forme d'information documentée;
f) être communiquée au sein de l'organisation; et
g) être mise à la disposition des parties intéressées, le cas échéant.

A.5.1.1 Politiques de sécurité de l'information
Un ensemble de politiques de sécurité de l'information doit être défini, approuvé par la direction, diffusé et communiqué aux salariés et aux tiers concernés.

7. Politique de sécurité de l'information

7.1 Introduction

Le système de management de la sécurité de l'information (SMSI) est un levier incontournable de la performance de notre organisation. Assurer la sécurité de l'information, c'est assurer la survie et la compétitivité de notre organisation.

Identifier les actifs sensibles et mettre en pratique des mesures de protection, de prévention, de détection, d'assurance et de correction nous permet d'assurer la confidentialité, l'intégrité et la disponibilité de nos actifs.

Les actifs sensibles sont :

- le personnel avec des autorités privilégiées
- les applications et systèmes essentiels
- les serveurs d'application
- les serveurs web
- les serveurs de base de données
- les réseaux
- les ordinateurs
- les projets en cours de développement

Les processus Apprécier les risques et Traiter les risques nous aident à définir :

- ce que l'on doit protéger
- de qui l'on doit protéger nos actifs
- comment protéger nos actifs en permanence

Les responsabilités et autorités du personnel pour établir, appliquer, surveiller, maintenir et améliorer la sécurité de l'information sont décrites dans les Descriptions de fonction.

7.2 Les politiques

La politique de sécurité de l'information est complétée par les politiques :

- appareils mobiles
- télétravail
- gestion des actifs
- contrôle d'accès
- mesures cryptographiques
- bureau propre et écran verrouillé
- protection contre les logiciels malveillants
- sauvegarde
- gestion des vulnérabilités
- gestion des réseaux
- développement
- relations avec les fournisseurs
- conformité
- données personnelles

La politique de sécurité de l'information est soutenue par nos processus, nos procédures et tous les enregistrements.

7.3 Les critères

La protection de l'information est caractérisée par les critères essentiels suivants :

- confidentialité - l'information est disponible seulement à des personnes autorisées et elle est préservée de toute divulgation, de tout accès ou de toute utilisation non autorisée
- intégrité - protection de l'exactitude et de la complétude de l'information
- disponibilité – l'information est accessible et utilisable à la demande par des personnes autorisées en temps voulu et de la manière requise
- authenticité – l'information est ce qu'elle revendique être
- imputabilité - possibilité d'attribuer la responsabilité d'un fait à une personne
- non-répudiation - l'impossibilité de nier la participation au traitement d'une information
- fiabilité - degré de confiance que l'on peut accorder
- traçabilité - information nécessaire pour identifier l'origine et le parcours

7.4 Les principes

Les principes de sécurité de l'information que nous respectons sont les suivants:

- le système de management de la sécurité de l'information (SMSI) est conforme aux lois, règlements et accords
- le SMSI est établi, maintenu et amélioré en continu selon des exigences de l'ISO 27001 et les meilleures pratiques
- la gestion des risques de sécurité de l'information est alignée aux objectifs stratégiques de notre organisation
- l'appréciation des risques les plus critiques est suffisamment détaillée
- le traitement des risques est proportionné
- le moindre privilège (accès restreint) concerne tout le personnel
- la séparation des tâches est strictement appliquée
- le personnel est :
    - formé et sensibilisé à la politique de sécurité de l'information
    - informé des mesures disciplinaires possibles

7.5 Les objectifs

Les objectifs à atteindre de notre système de management de la sécurité de l'information sont les suivants :

- maintenir la confidentialité de l'information
- garder l'intégrité de l'information
- respecter les exigences opérationnelles de disponibilité de l'information
- traiter en toute sécurité les informations sensibles
- augmenter la sensibilité, les connaissances et les compétences de l'ensemble du personnel sur :
    - l'engagement de soutenir la politique de sécurité de l'information
    - le respect des recommandations et restrictions de sécurité relatives :

  - à l'authentification
  - aux mots de passe
  - à l'utilisation des réseaux
  - à l'utilisation de la messagerie électronique
- signaler et enquêter tous les incidents de sécurité
- tester les plans de continuité d'activité
- encourager la participation de l'ensemble du personnel à l'amélioration du SMSI
- garantir le soutien quotidien du RSI au maintien du SMSI et de l'obligation de rendre compte régulièrement de la performance du SMSI à la direction