Sécurité de l'information

Historique

Toutes	Création	01/01/2022
Page	**Changement**	**Date**

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

1. Objet

La politique 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 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 sécurité de l'information s'applique :

- à l'ensemble du personnel
- à tous les départements de notre organisation
- à tous actifs numériques et papier de notre organisation
- à l'environnement de travail
- aux outils de gestion
- au travail avec les fournisseurs

Les règles et mesures de sécurité de l'information concernent l'accès physique aux locaux, le personnel, les moyens techniques et les logiciels.

4. Responsabilité

Le responsable sécurité de l'information (RSI) a l'autorité de l'écriture et de la mise à jour de la politique 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 : 2022

5.2 Politique

La direction doit établir une politique de sécurité de l'information qui :

a) est appropriée 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) inclut l'engagement de satisfaire aux exigences applicables en matière de sécurité de l'information ;

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 ;

g) être mise à la disposition des parties intéressées, le cas échéant.

A.5.1 Politiques de sécurité de l'information

Une politique de sécurité de l'information et des politiques spécifiques à une thématique doivent être définies, approuvées par la direction, publiées, communiquées et demandée en confirmation au personnel et aux parties intéressées concernés, ainsi que révisées à intervalles planifiés et si des changements significatifs ont lieu.

7. Politique 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 notre information et de nos actifs.

Les actifs sensibles sont, entre autres :

- 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.