GABARIT

POLITIQUE DE SÉCURITÉ DE L'INFORMATION

Objectif du document

Une politique de sécurité de l'information permet de démontrer l'engagement de la direction en matière de sécurité de l'information. Cette politique doit être communiquée à l'ensemble des utilisateurs sous une forme adéquate, accessible et compréhensible.

Les sections présentées dans ce gabarit devraient se retrouver dans votre politique de sécurité de l'information. Le contenu devra être adapté aux exigences des métiers et aux lois et règlements en vigueur.

Destinataire du document : gérant de l'entreprise ou responsable de la sécurité de l'information

Date de la dernière modification : 2016-12

Contenu de la Politique

Titre	**Politique de sécurité de l'information**
Date d'entrée en vigueur	[Date]
Dernière date de révision	[Date]
Fréquence de la révision	Ex. : Tous les 3 ans
Unité responsable	Ex. : Responsable de la sécurité de l'information
Instance d'approbation	Ex. : Conseil d'administration
Public visé	Ex. : Tous les employés

1. OBJECTIFS

La politique de sécurité de l'information (ci-après : la « Politique ») établit les exigences légales et règlementaires, et est conforme aux pratiques reconnues dans l'industrie.

Cette Politique établit les principes directeurs dans le but d'atténuer les risques tout en maintenant l'efficacité opérationnelle des activités de [NOM DE l'ENTREPRISE].

Cette Politique soutient la mise en œuvre et le maintien des mesures de protection de l'information réduisant à un niveau acceptable les risques susceptibles de porter atteinte à la disponibilité, à l'intégrité et à la confidentialité de l'information et pouvant causer des pertes financières ou des préjudices à la réputation de [NOM DE l'ENTREPRISE].

2. PRINCIPES DIRECTEURS

2.1.1. Considérant l'impact potentiel de l'exploitation d'une vulnérabilité de sécurité de l'information sur la confiance des clients ainsi que sur la réputation et la situation financière, la sécurité de l'information est la responsabilité de tous. Elle concerne l'ensemble des dirigeants, employés et consultants ainsi que tout fournisseur ou sous-traitant offrant des services ou ayant accès aux informations.

2.1.2. Les investissements en sécurité de l'information sont prévus par [NOM DES RESPONSABLES] dans le but de maintenir les risques de sécurité de l'information à un niveau acceptable pour [NOM DE L'ENTREPRISE].

2.1.3. Les mesures de protection de l'information à mettre en place sont proportionnelles aux risques de sécurité identifiés et déterminées en fonction de l'importance et des impacts potentiels sur les actifs à protéger.

2.1.4. La gestion des opérations de sécurité de l'information et des processus afférents est essentielle pour assurer la protection des actifs de [NOM DE l'ENTREPRISE] ainsi que pour détecter et contrer les principales menaces. La gestion des incidents de sécurité de l'information est en place pour traiter efficacement et rapidement les menaces s'étant matérialisées.

2.1.5. Une évaluation périodique des risques et des mesures de protection des actifs informatiques doit être effectuée.

2.1.6. La sécurité de l'information repose sur l'intégrité, la connaissance et la vigilance des employés. Les processus de gestion des ressources humaines et le programme de sensibilisation et de formation à la sécurité de l'information sont indispensables pour assurer un niveau approprié de compétence et d'expertise du personnel de [NOM DE l'ENTREPRISE] en matière de sécurité de l'information.

2.1.7. Les ententes et contrats dont [NOM DE l'ENTREPRISE] est partie prenante doivent contenir des dispositions écrites garantissant le respect,

par toutes les parties, des exigences en matière de sécurité et de protection de l'information.

2.1.8. [NOM DE l'ENTREPRISE] respecte la réglementation applicable et les exigences de l'industrie en matière de sécurité de l'information

3. RESPONSABILITÉS, APPLICATION ET RÉVISION

3.1. Rôles et responsabilités

5.1.1. Comité de direction de [NOM DE l'ENTREPRISE]

- nomme le responsable de la sécurité de l'information
- alloue les ressources financières associées à la sécurité de l'information
- communique l'importance de la sécurité de l'information aux dirigeants et aux employés de [NOM DE l'ENTREPRISE]
- appuie la mise en œuvre des mesures de protection.

- 5.1.2. Responsable de la sécurité de l'information
- évalue les risques et les menaces qui pourraient toucher les actifs de [NOM DE l'ENTREPRISE]
- assure la mise en place des mesures de protection
- sensibilise et forme les employés à la sécurité de l'information.

- 5.1.5. Gestionnaires
- adoptent les comportements visant à assurer la sécurité de l'information et sont des modèles en matière de sécurité de l'information auprès de leurs employés
- protègent les actifs TI sous leur responsabilité, le cas échéant
- prennent en charge les responsabilités qui leur sont attribuées dans les mesures de protection
- s'assurent que les employés sous leur responsabilité :
    - suivent et mettent en application le programme de sensibilisation et de formation à la sécurité de l'information
    - connaissent et respectent les mesures de protection
    - bénéficient uniquement des accès nécessaires à l'exercice de leurs fonctions.

5.1.6. Employés

- suivent le programme de sensibilisation et de formation à la sécurité de l'information et le mettent en application

- adoptent les comportements visant à assurer la sécurité de l'information
- respectent les mesures de protection de l'information.

3.2. Révision de la Politique

XX est responsable de réviser la présente Politique au minimum tous les XX ans.

4. ENTRÉE EN VIGUEUR

La Politique entre en vigueur le jour de son adoption.