[logo de l'organisation]

[nom de l'organisation]

POLITIQUE DE SECURITE DE L'INFORMATION

Code:	
Version:	
Date de la version:	
Créé par:	
Approuvée par:	
Niveau de confidentialité:	

Historique des modifications

Date	Version	Créé par	Description de la modification
JJ-MM-AAAA	0.1		Structure documentaire de base

Table des matières

1. But, portée et audience

L'objectif de cette politique de haut niveau est de définir le but, la direction, les principes et les règles de base pour le management de la sécurité de l'information.

La Politique est appliquée à l'ensemble du Système de Management de la Sécurité de l'Information (SMSI) tel que défini dans le Document du domaine d'application du SMSI.

Les utilisateurs de ce document sont tous les employés de [nom de l'organisation], de même que les tierces parties concernées.

2. Documents référencés

- Norme ISO/IEC 27001, clauses 5.2 et 5.3
- Document du domaine d'application du SMSI
- Méthodologie d'évaluation et de traitement des risques
- Déclaration d'applicabilité
- Liste des obligations statutaires, règlementaires et contractuelles
-
- [Politique de management de la continuité des activités]
- [Procédure de gestion des incidents]

3. Terminologie de base de la sécurité de l'information

Confidentialité - propriété de l'information selon laquelle elle n'est accessible uniquement qu'aux personnes ou systèmes autorisés

Intégrité - propriété de l'information selon laquelle elle n'est modifiée que par des personnes ou systèmes autorisés d'une manière contrôlée

Disponibilité - propriété de l'information selon laquelle elle n'est accessible que par des personnes autorisées quand elle est nécessaire

Sécurité de l'information - préservation de la confidentialité, de l'intégrité et de la disponibilité de l'information

Système de Management de la Sécurité de l'Information - la partie du système de management global qui s'occupe de planifier, mettre en œuvre, maintenir, revoir et améliorer la sécurité de l'information

4. Management de la sécurité de l'information

4.1. Buts et objectifs

Les objectifs généraux du système de management de la sécurité de l'information sont les suivants: de créer une meilleure image pour le marché et de réduire les dommages causés par des incidents potentiels; les buts sont alignés avec les objectifs métier de l'organisation, la stratégie et les plans d'affaires. [titre du poste] est responsable de la revue de ces objectifs généraux du SMSI et d'en déterminer de nouveaux.

Les objectifs pour les mesures individuelles de sécurité ou pour des groupes de mesures sont proposés par [liste de fonctions qui ont les autorisations nécessaires], et approuvés par [titre du poste] dans la Déclaration d'applicabilité.

Tous les objectifs doivent être révisés au moins une fois par an.

[nom de l'organisation] mesurera l'accomplissement de tous les objectifs. [titre du poste] est responsable de la définition d'une méthode pour la mesure de l'accomplissement des objectifs - cette mesure devra être réalisée au moins une fois par an et [titre du poste] analysera et évaluera les résultats des mesures et les rapportera à [la Direction] comme matière pour la revue de Direction.

4.2. Exigences de sécurité de l'information

Cette Politique et l'ensemble du SMSI doivent être en conformité avec les exigences légales et règlementaires applicables à l'organisation dans le domaine de la sécurité de l'information, ainsi qu'avec les obligations contractuelles.

Une liste détaillée de l'ensemble des exigences contractuelles et légales est fournie dans la Liste des exigences légales, règlementaires et contractuelles.

4.3. Mesures de sécurité de l'information

Le processus de sélection des mesures est défini dans la méthodologie d'évaluation et de traitement des risques.

Les mesures sélectionnées et leur état d'implémentation sont énumérés dans la Déclaration d'applicabilité.

4.4. Continuité des Activités

Le management de la continuité des activités est prescrit dans la Politique de management de la continuité des activités.

4.5. Responsabilités

Les responsabilités de base pour le SMSI sont les suivantes:

- [titre du poste] est responsable de veiller à ce que le SMSI soit implémenté conformément à cette Politique, et d'assurer toutes les ressources nécessaires.

- [titre du poste] est responsable de la coordination opérationnelle du SMSI ainsi que de rapporter au sujet de sa performance.
- [la direction] doit réviser le SMSI au moins une fois par an ou à chaque fois qu'un changement significatif survient, et préparer des compte-rendu de ces réunions. Le but de la revue de Direction est d'établir la pertinence, l'adéquation et l'efficacité du SMSI.
- [titre du poste] mettra en œuvre les formations et les programmes de sensibilisation sur la sécurité de l'information pour les employés.
- la protection de l'intégrité, de la disponibilité et de la confidentialité des actifs est de la responsabilité des propriétaires de chaque actif.
- tous les incidents ou vulnérabilités de sécurité doivent être rapportés à [titre du poste]

4.6. Communication de la Politique

[titre du poste] doit veiller à ce que tous les employés de [nom de l'organisation], ainsi que tous les tiers, soient familiers avec cette Politique.

5. Support pour l'implémentation du SMSI

Par la présente le [titre du poste ou organe de Direction dans le cadre du SMSI] déclare que l'implémentation du SMSI et son amélioration continue seront soutenues par des ressources adéquates afin d'atteindre tous les buts et objectifs fixés dans cette Politique, ainsi qu'à satisfaire toutes les exigences identifiées.

6. Validité et gestion documentaire

Ce document est valide dès le [date].

Le propriétaire de ce document est [titre du poste], qui doit vérifier et si nécessaire mettre à jour le document au moins une fois par an.

Pour évaluer l'efficacité et l'adéquation de ce document, les critères suivants doivent être considérés:

- nombre d'employés et de tiers qui ont un rôle dans le SMSI, mais qui ne sont pas familiers avec ce document
- non-conformité du SMSI avec les lois et les règlementations, avec les obligations contractuelles et avec d'autres documents internes de l'organisation
- inefficacité de l'implémentation et de la maintenance du SMSI
- responsabilités peu claires pour l'implémentation du SMSI

[titre du poste]
[nom]

_____
[signature]