[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 :	

Commented [AES1]: Pour apprendre à remplir ce document et pour consulter des exemples concrets de ce que vous devez rédiger, regardez ce tutoriel vidéo "How to Write the ISMS Policy According to ISO 27001".

Pour accéder au tutoriel : dans votre boîte de réception, consultez l'e-mail que vous avez reçu au moment de l'achat. Vous y trouverez un lien et un mot de passe qui vous permettront d'accéder au tutoriel vidéo.

Commented [AES2]: Remplissez tous les champs entre crochets [ ] dans ce document.

Commented [AES3]: Cet article vous aidera à comprendre le but d'une Politique de sécurité de l'information :

Information security policy – how detailed should it be?
https://advisera.com/27001academy/blog/2010/05/26/information-security-policy-how-detailed-should-it-be/

Commented [AES4]: Si vous avez besoin d'un document fournissant des règles détaillées sur la sécurité de l'information, alors utilisez le modèle de Politique de sécurité des technologies de l'information inclus dans le dossier "09_Annexe_A_de_la_norme_ISO_27001_Mesures_de_securite" de la Boîte à outils ISO 27001 et ISO 22301 Premium.

Commented [AES5]: Cet article vous aidera à comprendre le contenu d'une Politique de sécurité de l'information :

What is the ISO 27001 Information Security Policy, and how can you write it yourself?
https://advisera.com/27001academy/blog/2016/05/30/what-should-you-write-in-your-information-security-policy-according-to-iso-27001/

Commented [AES6]: Le système de codage des documents doit être aligné avec le système existant de l'organisation pour la codification des documents ; au cas où un tel système n'est pas en place, cette ligne peut être supprimée.

Historique des modifications

Date	Version	Créé par	Description de la modification
	0.1	Advisera	Structure documentaire de base

Table des matières

1. BUT, DOMAINE D'APPLICATION ET UTILISATEURS. 3

2. DOCUMENTS REFERENCES 3

3. TERMINOLOGIE DE BASE DE LA SECURITE DE L'INFORMATION 3

4. MANAGEMENT DE LA SECURITE DE L'INFORMATION 3

4.1. OBJECTIFS ET EVALUATIONS 4
4.2. EXIGENCES DE SECURITE DE L'INFORMATION 4
4.3. MESURES DE SECURITE DE L'INFORMATION 4
4.4. CONTINUITE DES ACTIVITES 4
4.5. RESPONSABILITES 4
4.6. COMMUNICATION DE LA POLITIQUE 5

5. SUPPORT POUR L'IMPLEMENTATION DU SMSI 5

6. VALIDITE ET GESTION DOCUMENTAIRE 5

1. But, domaine d'application et utilisateurs

Cette Politique de haut niveau a pour objectif de définir le but, l'orientation, 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], ainsi que les tierces parties concernées.

Commented [AES7]: Indiquez le nom de votre organisation.

2. Documents référencés

- Norme ISO/IEC 27001, clauses 5.2, 5.3, 6.2, 7.4 et A.6.3
- Document du domaine d'application du SMSI
- Méthodologie d'évaluation et de traitement des risques
- Déclaration d'applicabilité
- Liste des exigences légales, réglementaires, contractuelles et autres
- [Autres documents internes]
- [Politique de continuité des activités]
- [Procédure de gestion des incidents]

Commented [AES8]: Vous pouvez consulter un modèle pour ce document dans le dossier "04_Domaine_d_application_du_SMSI" de la Boîte à outils ISO 27001 et ISO 22301 Premium.

Commented [AES9]: Vous pouvez consulter un modèle pour ce document dans le dossier "06_Evaluation_et_traitement_des_risques" de la Boîte à outils ISO 27001 et ISO 22301 Premium.

Commented [AES10]: Vous pouvez consulter un modèle pour ce document dans le dossier "07_Applicabilite_des_mesures" de la Boîte à outils ISO 27001 et ISO 22301 Premium.

Commented [AES11]: Vous pouvez consulter un modèle pour ce document dans le dossier "03_Identification_des_exigences" de la Boîte à outils ISO 27001 et ISO 22301 Premium.

Commented [AES12]: Enumérez les autres documents internes de l'organisation associés à cette Politique - par exemple, le plan de développement stratégique, le plan commercial, les documents sur la gestion stratégique des risques, etc.

Commented [AES13]: Voir section 4.4

Commented [AES14]: Voir section 4.5

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

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

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

[illegible]

4. Management de la sécurité de l'information

4.1. Objectifs et évaluations

Les objectifs généraux du système de management de la sécurité de l'information sont les suivants : la création d'une meilleure image sur le marché et la réduction les dommages causés par des incidents potentiels ; les finalités sont conformes aux objectifs métier, à la stratégie et aux plans d'affaires de l'organisation. [Titre du poste] est chargé de réviser ces objectifs généraux du SMSI et d'en déterminer de nouveaux.

[illegible]

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

[illegible]

4.2. Exigences de sécurité de l'information

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

[illegible]

4.3. Mesures de sécurité de l'information

Le processus de sélection des mesures (protections) est défini dans la Méthodologie d'évaluation et de traitement des risques.

[illegible]

4.4. Continuité des activités

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

4.5. Responsabilités

Les responsabilités pour le SMSI sont les suivantes :

- [titre du poste] est chargé d'assurer la mise en œuvre du SMSI et sa maintenance conformément à la Politique, et d'assurer l'accès à toutes les ressources nécessaires.

Commented [AES15]: Si nécessaire, modifier et / ou ajouter d'autres objectifs tels que la conformité avec la règlementation / législation, le nombre d'incidents, la satisfaction des utilisateurs, etc. [illegible]

Commented [AES16]: Pour en savoir plus sur la conformité de l'activité à la norme ISO 27001, consultez cet article : [illegible]

Commented [AES17]: Pour en savoir plus sur l'importance des objectifs des mesures, consultez cet article : [illegible]

Commented [AES18]: Par ex. les objectifs pour les mesures relatives à l'informatique peuvent être proposées par le Chef du service informatique [illegible]

Commented [AES19]: Evaluer si cette fréquence est appropriée.

Commented [AES20]: Indiquez le nom de votre organisation.

Commented [AES21]: Vous pouvez consulter un modèle pour ce document dans le dossier [illegible]

Commented [AES22]: Enumérez également d'autres domaines qui sont réglementés par la législation locale - par ex. [illegible]

Commented [AES23]: Supprimer cette section si la continuité des activités n'est pas implémentée.

Commented [AES24]: Pour mieux comprendre les responsabilités de la direction, consultez cet article : [illegible]

Commented [AES25]: Membre de la direction.

- [titre du poste] est responsable de la coordination opérationnelle du SMSI ainsi que de la présentation concernant son efficacité.
- [direction] doit réviser le SMSI au moins une fois par an ou à chaque fois qu'une modification importante y est apportée, et préparer des comptes-rendus de ces réunions. Le but de la Revue de direction est d'établir la conformité, la pertinence et l'efficacité du SMSI.
- [titre du poste] mettra en œuvre les formations et les programmes de sensibilisation à 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 toutes les vulnérabilités de sécurité doivent être présentés à [titre du poste].
- [titre du poste] définira quels enseignements relatifs à la sécurité de l'information seront communiqués aux parties intéressées concernées (internes et externes), par qui et quand.
- [titre du poste] est responsable de l'adoption et de la mise en œuvre du Plan de formation et de sensibilisation, qui s'applique à toutes les personnes qui ont une fonction dans le management de la sécurité de l'information.

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, connaissent cette Politique.

5. Support pour l'implémentation du SMSI

Par la présente, le [titre du poste ou organe de direction dans le domaine d'application du SMSI] déclare que l'implémentation du SMSI et son amélioration constante seront soutenues par des ressources adéquates afin d'atteindre tous les objectifs fixés dans cette Politique et de satisfaire toutes les exigences identifiées.

6. Validité et gestion documentaire

Ce document est valide à compter du [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.

Lors de l'évaluation de l'efficacité et de la pertinence de ce document, les critères suivants doivent être considérés :

- le nombre d'employés et de tiers qui ont une fonction dans le SMSI, mais qui ne sont pas familiers avec ce document
- la non-conformité du SMSI avec les lois et les réglementations, avec les obligations contractuelles et avec d'autres documents internes de l'organisation

Commented [AES26]: Une ou plusieurs personnes ;

Commented [AES27]: Ce doit être un organe de direction dans le domaine d'application du SMSI - par ex.

Commented [AES28]: Ces éléments sont obligatoires

Commented [AES29]: Plusieurs personnes responsables

Commented [AES30]: Ou faire une référence à la Procédure de gestion des incidents.

Commented [AES31]: Ce programme vous permettra de former les employés, dès les sensibiliser à la sécurité et d'évaluer leurs connaissances :

Commented [AES32]: Il ne s'agit que de recommandations ;

Commented [AES33]: Indiquez le nom de votre organisation.

Commented [AES34]: Pour en savoir plus sur la fourniture des ressources, consultez cet article :

Commented [AES35]: Il ne s'agit que d'une recommandation ;

- l'inefficacité de l'implémentation et de la maintenance du SMSI
- les responsabilités peu claires pour l'implémentation du SMSI

[titre du poste]
[nom]

Commented [AES36]: La Politique de sécurité de l'information doit être approuvée par la direction dans le domaine d'application du SMSI.

[signature]

Commented [AES37]: Nécessaire uniquement si la Procédure pour le contrôle des documents et des enregistrements prescrit que les documents papier doivent être signés.