[Logo de l'organisation]

[Nom de l'organisation]

Commented [AES1]: Remplissez tous les champs entre crochets [ ] dans ce document.

POLITIQUE SUR L'UTILISATION DU CRYPTAGE

Commented [AES2]: Pour en savoir plus sur ce sujet, consultez cet article :

How to use cryptography according to ISO 27001 control A.8.24
https://advisera.com/27001academy/how-to-use-the-cryptography-according-to-iso-27001/

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

Commented [AES3]: 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

Ce document a pour but de définir les règles concernant l'utilisation des mesures et des clés cryptographiques, afin de protéger la confidentialité, l'intégrité, l'authenticité et la non-répudiation de l'information.

Ce document s'applique à l'ensemble du domaine d'application du Système de management de la sécurité de l'information (SMSI), c'est-à-dire à tous les systèmes et à toutes les informations utilisées dans le domaine d'application du SMSI.

Les utilisateurs de ce document sont [énumérer les titres de poste de personnes qui doivent se conformer à cette Politique].

Commented [AES4]: Par ex. direction, personnel informatique, utilisateurs à distance, etc.

2. Documents référencés

- Norme ISO/IEC 27001, clauses A.5.31 et A.8.24
- Politique de sécurité de l'information
- [Politique de classification des informations]
- [Liste des exigences légales, réglementaires, contractuelles et autres]

Commented [AES5]: Vous pouvez consulter un modèle pour ce document dans le dossier "05_Politiques_generales" de la Boîte à outils ISO 27001 et ISO 22301 Premium.

Commented [AES6]: Si vous ne disposez pas de cette Liste, alors énumérez dans ces crochets toutes les obligations légales et contractuelles relatives à l'utilisation de la cryptographie.

3. Utilisation de la cryptographie

3.1. Mesures cryptographiques

Conformément à la Politique de classification des informations, et aux obligations légales et contractuelles, l'organisation doit protéger les systèmes ou les informations individuelles au moyen des mesures cryptographiques suivantes :

[illegible]	***Outil cryptographique***	***Algorithme de cryptage***	[illegible]
[illegible]	*Jeton de sécurité*	*Algorithme AES*	[illegible]
[illegible]	*Logiciel cryptographique XXXX*	*Algorithme RSA*	[illegible]

Commented [AES7]: Cela comprend également les canaux de [illegible]

Commented [AES8]: Énumérer tout ce qui est réglementé par la Politique + les obligations légales et contractuelles + tous les systèmes utilisant déjà le cryptage - par ex. les connexions avec des ordinateurs distants, les paiements électroniques, etc.

[illegible]

[Titre du poste] est chargé de préparer des instructions détaillées concernant l'utilisation des outils cryptographiques mentionnées. [illegible]

3.2. Clés cryptographiques

[Titre du poste] est chargé de fixer les règles suivantes concernant la gestion des clés :

- création des clés cryptographiques publiques et privées
- activation et diffusion des clés cryptographiques
- définition du délai d'utilisation de clés et leur mise à jour régulière (conformément à l'évaluation des risques)
- [illegible]
- [illegible]
- [illegible]
- [illegible]

Les clés sont gérées par leurs propriétaires conformément aux règles mentionnées ci-dessus.

[illegible] [décrire la façon dont les clés seront protégées contre la perte, le changement ou la destruction]. En cas de perte, de corruption ou de destruction, les clés seront récupérées [décrire la méthode de récupération].

Commented [AES9]: Dans la plupart des cas, l'organisation ne sera pas en mesure de contrôler les clés cryptographiques parce [illegible]

Commented [AES10]: Selon les besoins, les responsabilités peuvent être étendues.

[illegible]

Commented [AES11]: Par ex. en les conservant dans un lieu à l'accès limité.

Commented [AES12]: Par ex. au moyen de copies de sauvegarde.

4. Gestion des enregistrements conservés sur la base de ce document

[illegible]	[illegible]	*Personne responsable de la conservation*	*Mesures pour la protection des enregistrements*	[illegible]
[illegible]	[illegible]	[titre du poste responsable de la gestion des clés]	Seul [titre du poste] dispose des droits d'accès à de tels enregistrements.	[illegible]
[illegible]	[illegible]	[titre du poste]	Seul [titre du poste] est autorisé à modifier et à publier les instructions.	[illegible]
[illegible]	[illegible]	[titre du poste]	Seul [titre du poste] est autorisé à modifier et à publier les règles.	[illegible]

Commented [AES13]: Modifiez ces enregistrements pour les faire correspondre aux pratiques de votre organisation. [illegible]

Commented [AES14]: Adaptez la durée dans cette colonne à [illegible]

Seul [titre du poste] peut accorder à d'autres employés l'accès à l'un des enregistrements mentionnés ci-dessus.

5. 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 semestre.

Commented [AES15]: Il ne s'agit que d'une recommandation ; ajuster si fréquence si différente.

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

- le nombre d'incidents liés à la perte, la compromission ou la destruction de clés cryptographiques
- le nombre de systèmes auxquels des mesures cryptographiques sont appliquées en méconnaissance des règles énoncées dans la présente Politique

[titre du poste]
[nom]

[signature]

Commented [AES16]: Nécessaire uniquement si la Procédure pour le contrôle des documents et des enregistrements prescrit que les documents papier doivent être signés.