[Logo de l'organisation]

[Nom de l'organisation]

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

POLITIQUE DES MOTS DE PASSE

Commented [AES2]: Il n'est pas nécessaire de rédiger un document distinct pour la Politique des mots de passe si les mêmes règles sont prescrites dans la Politique de sécurité des technologies de l'information et dans la Politique de contrôle d'accès.

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 fixer des règles destinées à sécuriser la gestion et l'utilisation des mots de passe.

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 lieux de travail et systèmes appartenant au domaine d'application du SMSI.

Les utilisateurs de ce document sont l'ensemble des employés de [nom de l'organisation].

Commented [AES4]: Indiquez le nom de votre organisation.

2. Documents référencés

- Norme ISO/IEC 27001, clauses A.5.16, A.5.17 et A.5.18
- Politique de sécurité de l'information
- Déclaration d'acceptation des documents du SMSI

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.

3. Obligations de l'utilisateur

Commented [AES6]: Supprimer cette section si les règles sont

Les utilisateurs doivent appliquer ces bonnes pratiques de sécurité lors de la sélection et de l'utilisation de mots de passe :

Commented [AES7]: Il ne s'agit que d'exemples des meilleures

- les mots de passe ne doivent pas être divulgués à d'autres personnes, y compris aux administrateurs système et à l'encadrement
- les mots de passe ne doivent pas être écrits sur papier, sauf si une méthode sécurisée a été approuvée par [titre du poste]
- des mots de passe fiables doivent être sélectionnés de la façon suivante :
  - en utilisant au moins 16 caractères
  - en utilisant au moins un caractère numérique
  - en utilisant au moins une lettre majuscule et au moins une lettre minuscule
- les mots de passe doivent être modifiés tous les 3 mois

- les mots de passe ne doivent pas être stockés dans un système de connexion automatisé (par ex. macro ou navigateur)
- [illegible]

Lorsque certaines des règles énumérées ci-dessus ne peuvent être appliquées (par ex. en raison de limites des systèmes), les pratiques existantes les plus fiables doivent être utilisées.

4. Gestion des mots de passe des utilisateurs

Commented [AES8]: Supprimer cette section si les règles sont [illegible]

Lors de l'attribution et de l'utilisation des mots de passe utilisateur, les règles suivantes doivent être respectées :

Commented [AES9]: Adapter ces règles en fonction des risques [illegible]

Commented [AES10]: Des règles distinctes peuvent être [illegible]

- en signant la Déclaration d'acceptation des documents du SMSI, les utilisateurs acceptent également l'obligation de préserver la confidentialité des mots de passe, conformément au présent document
- chaque utilisateur ne peut utiliser que le nom d'utilisateur unique qui lui a été attribué
- chaque utilisateur doit avoir la possibilité de choisir son propre mot de passe, quand cela est possible
- le mot de passe temporaire, utilisé pour la première connexion au système, doit être unique et fiable, tel que décrit ci-dessus
- les mots de passe temporaires doivent être communiqués à l'utilisateur de manière sécurisée et l'identité de l'utilisateur doit être vérifiée au préalable

Commented [AES11]: Vous pouvez apporter plus de précisions ici.

- le système de gestion des mots de passe doit demander à l'utilisateur de modifier le mot de passe temporaire lors de la première connexion au système
- le système de gestion des mots de passe doit demander à l'utilisateur de choisir des mots de passe fiables
- [illegible]

Commented [AES12]: Par ex. en envoyant un e-mail [illegible]

Commented [AES13]: Par ex. les trois derniers mots de passe.

Commented [AES14]: Par ex. en se connectant au système [illegible]

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 an.

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

- le nombre d'incidents relatifs à une mauvaise utilisation des mots de passe par des personnes non-autorisées
- le nombre d'incidents relatifs à la gestion inadéquate des mots de passe

[titre du poste]
[nom]

[signature]

Commented [AES15]: Il ne s'agit que d'une recommandation ; [illegible]

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