[Logo de l'organisation]

[Nom de l'organisation]

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

POLITIQUE DE CONTROLE D'ACCES

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

How to handle access control according to ISO 27001 https://advisera.com/27001academy/blog/2015/07/27/how-to-handle-access-control-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 des modifications
	0.1	Advisera	Structure documentaire de base

Table des matières

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

2. DOCUMENTS REFERENCES....3

3. CONTROLE D'ACCES....3

3.1. INTRODUCTION....3
3.2. PROFIL D'UTILISATEUR A....3
3.3. PROFIL D'UTILISATEUR B....4
3.4. GESTION DES PRIVILEGES....4
3.5. EXAMEN REGULIER DES DROITS D'ACCES....5
3.6. CHANGEMENT DE SITUATION OU RESILIATION DE CONTRAT....5
3.7. MISE EN ŒUVRE TECHNIQUE....6
3.8. AUTHENTIFICATION SECURISEE....6
3.9. GESTION DES MOTS DE PASSE DES UTILISATEURS....6

4. GESTION DES ENREGISTREMENTS CONSERVES SUR LA BASE DE CE DOCUMENT....7

5. VALIDITE ET GESTION DOCUMENTAIRE....7

1. But, domaine d'application et utilisateurs

Ce document a pour but de définir des règles d'accès aux différents systèmes, aux équipements, aux installations et aux informations, en fonction des exigences opérationnelles et de sécurité pour l'accès.

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, équipements, installations et informations utilisés dans le 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.5.15, A.5.16, A.5.17, A.5.18, A.8.2, A.8.3, A.8.4, A.8.5 et A.8.11
- Politique de sécurité de l'information
- Déclaration d'applicabilité
- [Politique de classification des informations]
- [Déclaration d'acceptation des documents du SMSI]
- [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]: 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 [AES7]: Si vous ne disposez pas de cette liste, alors énumérez dans ces crochets toutes les obligations légales et contractuelles relatives au contrôle d'accès.

3. Contrôle d'accès

3.1. Introduction

Le principe fondamental du contrôle d'accès prévoit que l'accès à tous les systèmes, les réseaux, les services et à toutes les informations est interdit, à moins d'une autorisation expresse accordée à des utilisateurs individuels ou à des groupes d'utilisateurs.

L'accès à tous les espaces physiques de l'organisation est autorisé, sauf à des zones pour lesquelles un privilège doit être accordé par la personne autorisée (section "Gestion des privilèges").

[redacted]

Commented [AES8]: Doit être supprimé si la Politique de [redacted]

3.2. Profil d'utilisateur A

Commented [AES9]: Adapter au système de nommage [redacted]

Le profil d'utilisateur A disposé des droits d'accès suivants :

Nom du système / réseau / service	[redacted]

Commented [AES10]: Peut-être précisé sur le niveau de l'ensemble du système ou pour des modules uniques.

Commented [AES11]: Indiquer s'ils comprennent les droits [redacted]

Les titres de poste suivants disposent de droits d'accès conformément au Profil d'utilisateur A :

- [titre du poste 1]
- [titre du poste 2]

Commented [AES12]: Enumérer tous les titres de poste.

3.3. Profil d'utilisateur B

Commented [AES13]: Des profils d'utilisateurs supplémentaires

Le profil d'utilisateur B dispose des droits d'accès suivants :

Nom du système / réseau / service	[Droits d'utilisateur]

Commented [AES14]: Peut-être précisé sur le niveau de

Commented [AES15]: Indiquer s'ils comprennent les droits

Les titres de poste suivants disposent de droits d'accès conformément au Profil d'utilisateur B :

- [titre du poste 1]
- [titre du poste 2]

3.4. Gestion des privilèges

Commented [AES16]: Supprimer cette section si la mesure

Les privilèges, en ce qui concerne les profils d'utilisateurs susmentionnés (octroi ou suppression des droits d'accès), sont attribués de la façon suivante :

Commented [AES17]: Ce tableau peut être remplacé par une

Nom du système / réseau / service / espace physique	[Qui est autorisé à accorder ou à supprimer les droits d'accès]	[Forme de processus d'autorisation]

Commented [AES18]: Par e-mail, décision écrite, oralement, via le système, etc.

Lors de l'attribution de privilèges, la personne responsable doit tenir compte des exigences opérationnelles et de sécurité pour l'accès (définies dans l'évaluation des risques), ainsi que de la classification des informations disponibles en vertu de tels droits d'accès, conformément à la Politique de classification des informations.

3.5. Examen régulier des droits d'accès

Commented [AES19]: Supprimer cette section si la mesure

Les propriétaires de chaque système et les propriétaires d'installations, pour lesquels des droits d'accès spéciaux sont nécessaires, doivent, aux intervalles suivants, examiner si les droits d'accès accordés sont conformes aux exigences opérationnelles et de sécurité :

Commented [AES20]: Adapter si nécessaire.

Nom du système / réseau / service / espace physique	[illegible]

Commented [AES21]: La fréquence doit être définie, en tenant

[illegible]

Commented [AES22]: Un formulaire, un rapport officiel, des

3.6. Changement de situation ou résiliation de contrat

Commented [AES23]: Supprimer cette section si la mesure

Lors d'un changement d'emploi ou à la résiliation du contrat, [titre du poste] doit immédiatement en informer les personnes responsables qui ont approuvé des privilèges en faveur de l'employé en question.

[illegible]

3.7. Mise en œuvre technique

La mise en œuvre technique de l'attribution ou de la suppression des droits d'accès est effectuée par les personnes suivantes :

Nom du système / réseau / service / espace physique	[illegible]

Les personnes inscrites dans ce tableau ne peuvent pas accorder ou retirer librement les droits d'accès, mais uniquement en vertu de profils d'utilisateurs définis dans la présente Politique et des demandes réalisées par des personnes autorisées à attribuer des privilèges.

3.8. Authentification sécurisée

[Titre du poste] s'assure qu'une procédure de connexion sécurisée est implémentée pour tous les équipements, systèmes et services.

3.9. Gestion des mots de passe des utilisateurs

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

- 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, comme décrit ci-dessus
- [illegible]

Commented [AES24]: Supprimer cette section si la mesure [illegible]

Commented [AES25]: Supprimer cette section si la Politique [illegible]

Commented [AES26]: Adapter ces règles en fonction des [illegible]

Commented [AES27]: Des règles distinctes peuvent être [illegible]

Commented [AES28]: Vous pouvez apporter plus de précisions ici.

Commented [AES29]: Il ne s'agit que d'une recommandation ; [illegible]

- si l'utilisateur demande un nouveau mot de passe, le système de gestion des mots de passe doit déterminer l'identité de l'utilisateur en [préciser comment]
- le système de gestion des mots de passe doit empêcher la réutilisation des [préciser combien] derniers mots de passe
- l'utilisateur doit confirmer la réception du mot de passe en [préciser comment]
- [illegible]

Commented [AES30]: Par ex. en envoyant un e-mail [illegible]

Commented [AES31]: Par ex. les trois derniers mots de passe.

Commented [AES32]: Par ex. en se connectant au système [illegible]

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 mise en œuvre technique]	Les enregistrements ne peuvent pas être modifiés ; seul [titre du poste] a le droit de conserver de tels enregistrements.	[illegible]
[illegible]	[illegible]	[titre du poste]	Seul [titre du poste] dispose des droits d'accès à de tels enregistrements.	[illegible]

Commented [AES33]: Modifiez ces enregistrements pour les faire correspondre aux pratiques de votre organisation. [illegible]

Commented [AES34]: Ajuster si nécessaire.

Commented [AES35]: Ajuster si nécessaire.

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

5. Validité et gestion documentaire

Ce document est valide à compter du [date].

[illegible]

Commented [AES36]: Il ne s'agit que d'une recommandation ; [illegible]

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

- le nombre d'incidents liés à l'accès non-autorisé à l'information
- la modification retardée des droits d'accès en cas de changement ou de cessation d'emploi / de contrat
- [illegible]
- [illegible]

[titre du poste]
[nom]

[signature]

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