[logo de l'organisation]

[nom de l'organisation]

Comment [DK1]: Tous les champs dans ce document marqués avec des crochets [ ] doivent être remplis.

POLITIQUE DE CONTROLE DES ACCES

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

Comment [DK2]: Le système de codage des documents devrait 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.

©2015 Ce modèle peut être utilisé par les clients de EPPS services Ltd. www.advisera.com en conformité avec l'accord de licence.

Historique des modifications

Date	Version	Créé par	Description des modifications
JJ-MM-AAAA	0.1	Dejan Kosutic	Structure documentaire de base

Table des matières

1. BUT, DOMAINE D'APPLICATION ET AUDIENCE 3

2. DOCUMENTS REFERENCES 3

3. CONTROLE D'ACCES 3

3.1. INTRODUCTION 3
3.2. PROFIL 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 STATUT OU RESILIATION DE CONTRAT 5
3.7. MISE EN ŒUVRE TECHNIQUE 5
3.8. GESTION DES MOTS DE PASSE 6

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

5. VALIDITE ET GESTION DOCUMENTAIRE 7

©2015 Ce modèle peut être utilisé par les clients de EPPS services Ltd. www.advisera.com en conformité avec l'accord de licence.

1. But, domaine d'application et audience

Le but de ce document est de définir des règles d'accès aux différents systèmes, aux équipements, aux installations et aux informations, en fonction des besoins d'affaires 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), soit à tous les systèmes, équipements, installations et informations utilisés dans le cadre du SMSI.

L'audience de ce document est l'ensemble des employés de [nom de l'organisation].

2. Documents référencés

- Norme ISO/IEC 27001, clauses A.9.1.1, A.9.1.2, A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.5, A.9.2.6, A.9.3.1, A.9.4.1, A.9.4.3
- 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]

Comment [DK3]: Si vous n'avez pas cette liste, alors énumérer dans cette partie toute la législation et les contrats qui contiennent des exigences en matière de contrôle d'accès.

3. Contrôle d'accès

3.1. Introduction

Le principe de base est que l'accès à tous les systèmes, les réseaux, les services et les informations est interdit, sauf autorisation expresse permise à des utilisateurs ou groupes d' utilisateurs individuels. Il devrait y avoir une procédure d'enregistrement de l'utilisateur pour chaque système et service.

Comment [D4]: Supprimer ceci si la mesure [illegible] dans la Déclaration d'applicabilité.

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

Cette Politique précise les règles d'accès aux systèmes, services et installations, tandis que la [Politique de classification des informations] définit les règles d'accès aux documents et enregistrements individuels.

Comment [D5]: Doit être supprimé si la Politique de classification des informations n'est pas documentée.

3.2. Profil utilisateur A

Comment [D6]: Adapter au système de [illegible]

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

Nom du système / réseau / service	[illegible]

Comment [D7]: Peut être spécifié sur le niveau [illegible] simples.

Comment [D8]: Indiquer s'ils comprennent les [illegible] spécifiques.

©2015 Ce modèle peut être utilisé par les clients de EPPS services Ltd. www.advisera.com en conformité avec l'accord de licence.

Les postes suivants ont les droits d'accès selon le Profil d'utilisateur A:

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

3.3. Profil d'utilisateur B

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

Nom du système / réseau / service	[illegible]

Les postes suivants ont les droits d'accès selon le Profil d'utilisateur B:

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

3.4. Gestion des privilèges

[illegible] (octroi ou suppression des droits d'accès) sont attribués de la façon suivante:

Nom du système / réseau / service / zone physique	***Qui est autorisé pour l'octroi ou le retrait des droits d'accès***	[illegible]

Comment [D9]: Inscrire tous les postes. Il peut [illegible] l'embauche.

Comment [D10]: Des profils d'utilisateurs [illegible]

Comment [D11]: Peut être spécifié sur le niveau [illegible] spécifiques.

Comment [D12]: Indiquer s'ils comprennent les droits pour la lecture, l'écriture, la suppression, la modification et / ou l'exécution de fonctions spécifiques.

Comment [D13]: Supprimer cette section si la mesure A.9.2.3 est marquée comme inapplicable dans la Déclaration d'applicabilité.

Comment [DK14]: Ce tableau peut être [illegible] propriétaires respectifs.

Comment [D15]: Par e-mail, décision écrite, [illegible] devrait y avoir un enregistrement.

©2015 Ce modèle peut être utilisé par les clients de EPPS services Ltd. www.advisera.com en conformité avec l'accord de licence.

Lors de l'attribution de privilèges, la personne responsable doit tenir compte des besoins de [illegible] Politique de classification des informations.

3.5. Examen régulier des droits d'accès

Les propriétaires de chaque système et les propriétaires d'installations pour lesquels des droits [illegible] d'accès accordés sont en ligne avec les exigences opérationnelles et de sécurité:

[illegible] *service / zone physique*	***Intervalles de révision régulière***

Chaque révision doit être enregistrée [préciser comment les enregistrements sont conservés].

3.6. Changement de statut ou résiliation de contrat

Lors d'un changement d'emploi ou d'une cessation d'emploi, [titre du poste] doit immédiatement en [illegible]

[illegible] et installations, ou à l'expiration du contrat, le propriétaire du contrat doit immédiatement informer les personnes responsables qui ont approuvé des privilèges pour les parties externes en question.

[illegible] contractuelle doivent immédiatement être supprimés ou modifiés par des personnes responsables au sens de la section suivante.

3.7. Mise en œuvre technique

[illegible] des droits d'accès est effectuée par les personnes suivantes:

Comment [D16]: Supprimer cette section si la mesure A.9.2.5 est marquée comme inapplicable dans la Déclaration d'applicabilité.

Comment [D17]: [illegible]

Comment [D18]: La fréquence devrait être [illegible] d'évaluation des risques.

Comment [D19]: Un formulaire, rapport officiel, notes écrites à la main, etc., peuvent être utilisés.

Comment [DK20]: Supprimer cette section si la mesure A.9.2.6 est marquée comme inapplicable dans la Déclaration d'applicabilité.

©2015 Ce modèle peut être utilisé par les clients de EPPS services Ltd. www.advisera.com en conformité avec l'accord de licence.

[illegible] *service / zone physique*	***Personne responsable de la mise en œuvre***

Les personnes inscrites dans ce tableau peuvent ne pas accorder ou retirer librement les droits d'accès, mais seulement sur la base de profils d'utilisateur définis dans la présente Politique, et des demandes par des personnes autorisées pour l'attribution des privilèges.

3.8. Gestion des mots de passe

Lors de l'allocation et 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 conserver les mots de passe confidentiels, tel que prescrit par le présent document
- chaque utilisateur ne peut utiliser que son propre nom d'utilisateur alloué de manière unique
- 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 sur le système doit être unique et fort, comme 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 auparavant
- le système de gestion des mots de passe doit obliger l'utilisateur à changer le mot de passe temporaire à la première connexion au système
- le système de gestion des mots de passe doit demander à l'utilisateur de choisir des mots de passe forts
- le système de gestion des mots de passe doit obliger les utilisateurs à changer leurs mots de passe tous les trois mois
- si un utilisateur demande un nouveau mot de passe, le système de gestion des mots de passe doit déterminer l'identité de l'utilisateur par [préciser comment]
- l'utilisateur doit confirmer la réception du mot de passe par [préciser comment]
- le mot de passe ne doit pas être visible sur l'écran lors de la connexion
- si un utilisateur entre un mot de passe incorrect trois fois de suite, le système doit bloquer le compte de l'utilisateur en question
- les mots de passe créés par le fabricant de logiciel ou de matériel doivent être modifiés lors de l'installation initiale
- Les fichiers contenant les mots de passe doivent être stockés séparément des données du système de l'application

Comment [D21]: Supprimer cette partie si la Politique des mots de passe constitue un document séparé.

Comment [D22]: Adapter ces règles en fonction des risques évalués.

Comment [DK23]: Des règles distinctes peuvent être définies pour les mots de passe administrateur et utilisateur.

Comment [D24]: Plus de détails peuvent être fournis ici.

Comment [D25]: Par exemple en envoyant un e-mail demandant à l'utilisateur d'effectuer une action, etc.

Comment [D26]: Par exemple en se connectant sur le système dans un intervalle de temps, etc.

©2015 Ce modèle peut être utilisé par les clients de EPPS services Ltd. www.advisera.com en conformité avec l'accord de licence.

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

Nom de l'enregistrement	Lieu de conservation	Personne responsable de la conservation	Mesures pour la protection des enregistrements	Temps de rétention
[Enregistrement d'attribution de privilèges (sous forme électronique - message e-mail)]	[dossier intranet]	[titre du poste responsable de la ma mise en œuvre technique]	Les enregistrements ne peuvent pas être modifiés; seul [titre du poste] a le droit de stocker ces enregistrements	Les enregistrements sont stockés pour une période de 3 ans
[Enregistrements de l'examen régulier des droits d'accès]	[[titre du poste] de l'ordinateur / [titre du poste] de l'armoire]	[titre du poste]	Seul [titre du poste] a les droits d'accès à de tels enregistrements	Les enregistrements sont stockés pour une période de 3 ans

Comment [D27]: Ajuster comme il se doit.

Comment [D28]: Ajuster comme il se doit.

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

5. Validité et gestion documentaire

Ce document est valide dès le [date].

Le propriétaire de ce document est [titre du poste], [illegible] document au moins une fois tous les six mois.

Comment [DK29]: Ceci est juste une recommandation; ajuster comme il se doit.

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

- [illegible]
- le changement retardé des droits d'accès en cas de changement ou de cessation d'emploi / de contrat
- [illegible]
- le niveau de confusion concernant les responsabilités pour la mise en œuvre de ce document

[titre du poste]
[nom]

©2015 Ce modèle peut être utilisé par les clients de EPPS services Ltd. www.advisera.com en conformité avec l'accord de licence.

[signature]

Comment [DK30]: Seulement nécessaire si la Procédure pour le Contrôle des Documents et des Enregistrements prescrit que ces documents papier doivent être signés.

©2015 Ce modèle peut être utilisé par les clients de EPPS services Ltd. www.advisera.com en conformité avec l'accord de licence.