Politique de gestion des droits d'accès

 Modèle

# Autorité et révision

## Contrôle et révision des documents

|  |  |
| --- | --- |
| **Vérification des documents**  |  |
| Auteur  |  |
| Propriétaire |  |
| Date de création |  |
| Dernière révision par  |  |
| Date de la dernière révision |  |

.

## Gestion des versions

|  |  |  |  |
| --- | --- | --- | --- |
| **Version**  | **Date d'approbation** | **Approuvé par**  | **Description du changement** |
|  |  |  |  |

# Intro

Au sein de **[l’organisation]** , la gestion des accès est une composante essentielle de la sécurité qui détermine qui a accès à certaines données, applications et autres ressources numériques, et dans quelles circonstances. Ces politiques de gestion des accès sécurisent les environnements numériques de la même manière que les clés et les listes d'invités sécurisent les espaces physiques. En d'autres termes, elles permettent aux bonnes personnes d'entrer et empêchent les autres d'entrer. Ces politiques reposent sur des techniques telles que l'authentification et l'autorisation. Celles-ci permettent à **[l'organisation]** de vérifier que les utilisateurs sont bien ceux qu'ils prétendent être et que l'accès approprié leur a été accordé, en fonction du contexte (appareil, emplacement, fonction, etc.).

# Le présent document fait partie d'un ensemble de documents destinés à aider [l'organisation] à mettre en place une stratégie solide en matière de cybersécurité.

# Gestion de l'accès

 **[L'organisation]** applique le principe de l'accès minimal. Cela signifie que chaque utilisateur interne ou externe de **[l'organisation]** se voit accorder un accès exactement suffisant aux informations et aux systèmes dont il a besoin pour exercer correctement ses fonctions. En outre, **[l'organisation]** préfère mettre en œuvre et appliquer, dans la mesure du possible, une authentification multifactorielle (AMF) standard.

L'accès à distance aux systèmes critiques et confidentiels de **[l'organisation]** à partir d'un lieu non fiable, tel que le domicile de l'employé ou le bureau du client, doit être limité aux utilisateurs désignés. Les ordinateurs portables de **[l'organisation]** sont équipés de paramètres permettant d'établir une connexion VPN aux systèmes de **[l'organisation]**.

Les accès accordés sont vérifiés à intervalles réguliers et modifiés si nécessaire. Les ajustements relatifs à l'accès, y compris le travail à distance, sont communiqués en temps utile au **[responsable au sein de l'organisme]** au moyen d'unformulaire de création/modification de compte (ACMF) ou d'un formulaire de suppression de compte (ARF) **(voir ANNEXE 1 Formulaires**).

# Gestion des comptes

## Comptes d'utilisateurs

Les comptes d'utilisateurs sont un moyen courant d'authentification. Les règles suivantes s'appliquent aux comptes d'utilisateurs pour l'accès aux systèmes critiques et confidentiels :

* doit être unique et personnelle.
* doivent être protégés par un mot de passe, comme décrit dans la politique relative aux mots de passe.
* les nouveaux comptes d'utilisateur pour les employés ne peuvent être demandés que par une personne autorisée et traités.
* doivent être retirés lorsqu'ils deviennent obsolètes (par exemple, à la fin du contrat).

## Comptes privilégiés

L'attribution de comptes à privilèges (par exemple, administrateur de domaine, super utilisateur et root) doit être limitée. Les comptes à privilèges ne doivent être utilisés que lorsque l'accès privilégié est nécessaire. Les propriétaires de ces comptes doivent utiliser un compte non privilégié pour les activités normales de l'utilisateur. Par exemple, les administrateurs système ne doivent pas utiliser leur compte d'administrateur de domaine pour gérer leur courrier électronique.

Le nom de ce compte ne doit pas divulguer d'informations sur les privilèges étendus du compte, ceci afin d'éviter les abus.

Pour les comptes privilégiés des systèmes critiques et confidentiels auxquels on accède à partir de réseaux non fiables tels que l'internet, il convient d'utiliser l'authentification multifactorielle.

## Comptes partagés

L'utilisation de comptes partagés doit être évitée. S'il n'est pas possible de l'empêcher raisonnablement, l'utilisation des comptes partagés doit être contrôlée. Des contrôles doivent être mis en place pour

* Savoir qui peut utiliser le compte.
* Contrôle de l'utilisation du compte.
* Processus de changement de mot de passe et communication du nouveau mot de passe.
* Prévenir les abus, par exemple en cas de résiliation du contrat.

## Comptes du personnel externe et des entreprises externes

Les contrôles supplémentaires suivants doivent être effectués pour les comptes du personnel externe :

* Les comptes doivent être facilement identifiables comme étant destinés au personnel externe, par exemple en ajoutant un préfixe au nom du compte ou en le mentionnant dans une description.

Les comptes doivent être révoqués à la fin du contrat. Si ce processus ne peut être entièrement garanti, le compte doit automatiquement expirer tous les **[3 mois],** sauf si le renouvellement est officiellement approuvé.

## Comptes de service pour la communication entre les systèmes

Les contrôles supplémentaires suivants doivent être présents pour les comptes de service et les comptes de communication de machine à machine :

* Les comptes doivent être facilement identifiables en tant que comptes de service, par exemple en ajoutant un préfixe au nom du compte ou en le mentionnant dans une description.
* Là encore, le principe de l'accès minimal s'applique.
* L'utilisation interactive des comptes de service doit être évitée.

# Authentification et autorisation

**Microsoft Active Directory (AD)** est une solution centralisée d'authentification et d'autorisation qui permet de gérer les droits et les paramètres de sécurité au sein d'un réseau. AD est intégré à l'environnement Windows et permet de déléguer la gestion de l'environnement Windows **[de l'organisation].**

## Authentification

* Grâce à une procédure de connexion sécurisée, il devrait être possible de contrôler l'accès aux systèmes et aux applications.
* Le **[responsable informatique]** doit enregistrer et contrôler chaque tentative de connexion, qu'elle soit réussie ou non.
* Les mots de passe initiaux doivent être transmis directement et en toute sécurité à l'utilisateur.
* Ces mots de passe doivent être modifiés immédiatement.
* L'authentification multifactorielle doit être utilisée lorsque cela est approprié et possible.
* Le compte de l'utilisateur doit être suspendu pour une période prédéterminée si l'utilisateur effectue un nombre prédéterminé de tentatives d'authentification infructueuses **[3 tentatives]** au cours d'une période prédéterminée **[5 minutes].**
* L'accès au système devrait être suspendu lorsque le compte n'a pas été utilisé pendant une période prédéterminée **[par exemple 90 jours].**

## Autorisation

* L'octroi ou le refus d'accès aux systèmes d'information ne peut être demandé en temps utile qu'au moyen d'un formulaire ACMF / ARF. (voir ANNEXE 1 Formulaires)
* Cet accès ne peut être demandé que par le responsable RH ou le N+1 de la personne concernée.
* Avant que l'accès ne soit accordé, le **[responsable de l'organisation]** doit donner son accord formel. Le **[responsable informatique]** doit accorder, mettre à jour et supprimer les droits d'accès.
* Les groupes d'autorisation sont utilisés autant que possible et l'accès est accordé en fonction des rôles.