[Nom de l’entreprise]

Politique de mise en œuvre des contrôles d’accès et des autorisations (politique utilisateur)

[Insérer la date]

**Avis de non-responsabilité**

**Instructions** : CyberSécuritaire Canada a élaboré ce modèle pour que vous puissiez l’utiliser en relation avec les exigences de certification du contrôle de sécurité **Offrir de la formation aux employés pour les sensibiliser**. Il fournit des conseils sur la manière dont les informations peuvent être organisées et documentées en vue de la certification. CyberSécuritaire Canada ne garantit pas que l’utilisation de ce modèle mène nécessairement à l'obtention de la certification. Les entreprises ne sont pas forcées d'utiliser ce modèle et peuvent fournir la ou les exigences de certification dans le format documenté qui leur convient le mieux.

# Directives pour le modèle

**Instructions**:L’objectif de ce modèle est d’aider les utilisateurs à répondre aux exigences de certification du contrôle de sécurité **Mettre en œuvre des contrôles d’accès et des autorisations** de CyberSécuritaire Canada.

Les instructions sont indiquées en caractères bleus dans chaque section de ce modèle. Une fois le modèle terminé, supprimer ces instructions.

Il est recommandé aux utilisateurs d’examiner le module d’apprentissage en ligne intitulé **Mettre en œuvre des contrôles d’accès et des autorisations** et l’exemple complet de cette politique. **Fin des instructions**.

# Historique des révisions

Il est de bonne pratique pour les entreprises de réviser et de mettre à jour leurs politiques régulièrement.

La politique de mise en œuvre des contrôles d’accès et des autorisations a été modifiée comme suit :

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Modification | Modifier |
| [Date] | [Version du document] | [Description des changements] | [Nom de l'éditeur] |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# Portée

**Instructions**:Insérer votre déclaration de portée ou utiliser l’exemple fourni.

Cette politique vise tous les employés, entrepreneurs et affiliés de [Nom de l’entreprise] qui ont un compte général ou administratif sur les appareils et systèmes de [Nom de l’entreprise].

# Tous les comptes

**Instructions**:Insérer vos déclarations de politique de tous les comptes ci-dessous; vous pouvez également utiliser l'exemple fourni.

1. Les comptes disposent uniquement des outils administratifs de base.
2. L’accès de partage du réseau est limité et contrôlé.
3. Les utilisateurs doivent être authentifiés avant d’avoir accès à un compte.
4. Tous les utilisateurs disposeront uniquement des privilèges d’accès au compte en fonction de leur rôle.
5. Les comptes sont supprimés lorsque les employés quittent l’entreprise.

# Comptes généraux

**Instructions**: Il est important de s'assurer que les comptes utilisateur généraux n'offrent pas les fonctions de compte administrateur. Les comptes administrateur doivent être limités à l'exécution d’activités administratives seulement. La vérification des courriels et la navigation sur Internet sont des exemples d'activités qui ne doivent pas être effectuées lorsque l’utilisateur est connecté en tant qu’administrateur.

Insérer vos déclarations de politique générale des comptes généraux ci-dessous. Vous pouvez également utiliser l'exemple ci-dessous.

Dresser la liste des activités que peuvent effectuer les utilisateurs de comptes généraux.

Indiquer clairement que les utilisateurs de compte général disposent de privilèges d’accès inférieurs à ceux d’un compte administrateur.

Les comptes généraux sont administrés par [Nom de l’entreprise] et n’ont aucun droit d'administrateur.

# Comptes d’administrateur

**Instructions**:

* Déterminer les logiciels/systèmes informatiques auxquels s'appliquent les comptes administrateur.
* Identifier les personnes de votre entreprise qui auront un compte administrateur.
* Déterminer et énumérer les pouvoirs et les activités d'un utilisateur de compte administrateur.
* Insérer vos déclarations de politique générale des comptes administrateur ci-dessous. Vous pouvez également utiliser l'exemple ci-dessous.
1. Droits administratifs accordés pour :
	1. Désactiver ou réinitialiser les mises à jour logicielles.
	2. Désactiver les anti-maliciels.
	3. Modifier les paramètres du logiciel.
2. Les utilisateurs du compte administrateur seront limités au personnel du service des TI.
3. Les comptes administrateur sont limités à des activités administratives. Les utilisateurs qui disposent d'un compte administrateur doivent également disposer d'un compte général à des fins professionnelles.

# Gestion des identités et des accès

**Instructions**: Les entreprises peuvent utiliser des systèmes de contrôle d'autorisation centralisés pour la gestion de leurs comptes utilisateur. Si votre entreprise n'utilise pas ce type de système, indiquer que cette section n'est pas applicable.

Insérer vos déclarations de politique relatives à l'identification et à la gestion des accès aux comptes administrateur.

# Application de la loi

**Instructions**:Insérer vos déclarations d’application ci-dessous ou utiliser l’exemple fourni.

Il incombe au [insérer] d’assurer le respect de cette politique et d'accorder aux utilisateurs les comptes et privilèges d’accès appropriés correspondant à leur rôle et leurs responsabilités. Il incombe aux gestionnaires et chefs d'équipe de vérifier les privilèges d’accès des comptes de leurs employés auprès du [insérer le titre/nom du responsable d’assurer le respect de cette politique].

# Exigences de certification supplémentaires

## Personnel autre que des TI disposant de droits d'administrateur

|  |
| --- |
| **Instructions**: Décrire les situations pour lesquelles des personnes qui ne sont pas associées aux TI disposent de droits d'administrateur et expliquer pourquoi elles doivent posséder ce niveau d’autorité. |

## Gestion des comptes

|  |
| --- |
| **Instructions**: Décrire comment votre entreprise entend examiner les comptes pour s'assurer que ceux des employés qui ont quitté l’entreprise sont suspendus ou supprimés. De plus, donner un aperçu de la façon dont les comptes sont régulièrement examinés pour s'assurer que chaque personne dispose des privilèges et des fonctionnalités appropriés au poste qu’elle occupe. |