

1. **Demande d'Accès:**

1.1. **Initiation:**

- Toute demande d'accès aux systèmes d'information et aux données doit être initiée via un formulaire de demande d'accès, dûment rempli et signé par le demandeur et son supérieur hiérarchique.

1.2. **Validation Initiale:**

- Le service des Ressources Humaines valide l'identité du demandeur et la légitimité de la demande en fonction du poste du demandeur.

2. **Évaluation des Besoins:**

2.1. **Analyse des Besoins:**

- Le service informatique (IT) évalue les besoins spécifiques en accès du demandeur en collaboration avec le chef du département concerné.

2.2. **Niveau d'Accès:**

- Détermination du niveau d'accès nécessaire (lecture seule, lecture-écriture, accès administrateur, etc.).

3. **Approvisionnement des Accès:**

3.1. **Configuration des Accès:**

- Le service IT configure les accès du demandeur en accord avec le niveau d'accès déterminé.

3.2. **Enregistrement:**

- Enregistrement des accès dans le système de gestion des identités et des accès.

4. **Révision de la Sécurité:**

4.1. **Validation des Configurations:**

- Vérification que les configurations d'accès respectent les politiques de sécurité de l'entreprise.

4.2. **Test d'Accès:**

- Test des accès pour s'assurer qu'ils fonctionnent comme prévu et n'octroient pas d'accès au-delà de ce qui est nécessaire.

5. **Formation et Sensibilisation:**

5.1. **Formation sur la Sécurité:**

- Fourniture d'une formation sur les responsabilités en matière de sécurité des données et les bonnes pratiques.

5.2. **Sensibilisation aux Politiques:**

- Sensibilisation aux politiques de l'entreprise en matière de gestion des accès et de sécurité des données.

6. **Communication:**

6.1. **Notification d'Accès:**

- Notification au demandeur et à son supérieur des accès qui ont été configurés.

6.2. **Documentation:**

- Documentation des accès octroyés dans le registre d'accès.

7. **Révision Périodique:**

7.1. **Audit des Accès:**

- Revue périodique des accès pour s'assurer qu'ils restent appropriés et conformes aux politiques de sécurité.

7.2. **Mise à jour des Accès:**

- Mise à jour des accès en cas de changement de rôle ou de responsabilités du demandeur.

8. **Révocation des Accès:**

8.1. **Demande de Révocation:**

- En cas de départ ou de changement de poste, le supérieur hiérarchique ou le service RH initie une demande de révocation ou de modification des accès.

8.2. **Exécution de la Révocation:**

- Le service IT exécute la révocation ou la modification des accès comme demandé et documente ces changements dans le système de gestion des identités et des accès.

Cette procédure d'autorisation des accès a été conçue pour garantir que l'accès aux données et aux systèmes d'information de [Nom de l'Entreprise] est contrôlé et sécurisé, conformément aux politiques de l'entreprise et aux réglementations en vigueur.

Documents Annexes:

- Annexe A: Formulaire de Demande d'Accès
- Annexe B: Politique de Gestion des Accès de [Nom de l'Entreprise]
- Annexe C: Guide de Bonnes Pratiques en Sécurité des Données

Références:

- Norme ISO/IEC 27001:2013 – Systèmes de management de la sécurité des informations.
- Loi camerounaise sur la protection des données personnelles et la vie privée.